# Gestion de la flotte de serveurs Microsoft Windows avec AWS Directory Service

*Mai 2015*

# 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 5

Challenges liés à la gestion d'une flotte de serveurs 5

Présentation d'AWS Directory Service 7

- AD Connector 8
- Simple AD 8

Joindre les instances Amazon EC2 pour Windows à un domaine AWS 9

Exemple Amazon EC2 pour Windows 9

- Utiliser les filtres WMI pour appliquer les objets Stratégie de groupe 11
- Joindre les instances au domaine AWS Directory Service 12
- Vérifier que les instances sont configurées correctement 18

Conclusion 20

# Résumé

Que ce soit sur site ou dans le cloud, la gestion d'une importante flotte de serveurs Windows Server peut être une tâche difficile. Active Directory relève le plupart des défis en centralisant les informations d'identification et en appliquant les configurations serveur, entre autres. Avec le lancement du service AWS Directory, vous pouvez connecter votre domaine Active Directory existant au cloud AWS à l'aide d'AD Connector ou lancer un nouveau domaine autonome dans AWS à l'aide d'un répertoire Simple AD.

Le livre blanc décrit comment le service AWS Directory Service et l'API Amazon EC2 SSM (Simple Systems Manager) peuvent être utilisés pour gérer votre flotte Windows Server dans Amazon EC2.

# Introduction

L'utilisation d'un annuaire tel que Microsoft Active Directory simplifie les tâches associées à la gestion des informations d'identification et à la configuration des serveurs. Il fournit un référentiel centralisé pour stocker les informations d'identification, ce qui permet une authentification unique entre tous les serveurs, ainsi qu'une intercommunication entre les serveurs. Avec les objets Stratégie de groupe (GPO) d'Active Directory, vous pouvez gérer différentes options de configuration pour des milliers de serveurs.

Le livre blanc fournit une vue d'ensemble du service AWS Directory et explique comment joindre les instances Amazon Elastic Compute Cloud (Amazon EC2) à un domaine AWS.

# Challenges liés à la gestion d'une flotte de serveurs

Que ce soit sur site ou dans le cloud, la gestion d'une flotte de serveurs peut être une tâche difficile. Chaque serveur possède un ensemble unique d'informations d'identification et le suivi de la correspondance entre informations d'identification et serveur est fastidieux. L'intercommunication entre les membres de la flotte nécessite le stockage ou la saisie d'informations d'identification pour les serveurs qui doivent communiquer entre eux, et la mise à jour des informations d'identification implique d'accéder à chaque serveur où les informations d'identification modifiées sont stockées. La configuration de chaque serveur constitue aussi un défi. Même si certaines options de configuration peuvent se retrouver sur tous les serveurs, d'autres options peuvent ne s'appliquer qu'à un rôle serveur. Garantir que la bonne configuration est appliquée nécessite que vous vous connectiez à chaque serveur avec des informations d'identification uniques pour valider les paramètres.

Ces difficultés ne disparaissent pas lorsque vous exécutez votre flotte sur EC2. De fait, le modèle AWS de paiement à l'utilisation peut rendre la gestion de la flotte plus complexe, car les instances sont ajoutées et supprimées dynamiquement. L'ajout de quelques instances à un groupe de serveurs déjà en cours d'exécution peut nécessiter que vous vous connectiez à chaque instance afin de stocker les informations d'identification pour communiquer avec le serveur. Par exemple, une modification du mot de passe des informations d'identification utilisées pour communiquer avec SQL Server entraîne une interruption jusqu'à ce que les informations d'identification stockées soient mises à jour. Même une simple modification de configuration, comme le changement de la taille des journaux d'événements, nécessite que vous vous connectiez manuellement à chaque instance pour procéder à la modification de la configuration. Quelle que soit la taille de la flotte, les erreurs consécutives aux modifications manuelles de la configuration et les interruptions peuvent impacter de façon négative la satisfaction des utilisateurs. La procédure pour vous assurer que vos instances sont configurées correctement et que vos informations d'identification sont documentées doit être rigoureusement suivie, parce qu'une erreur pourrait entraîner une défaillance de l'application et la frustration des utilisateurs.

Active Directory aide à relever certains de ces défis. Il fournit un référentiel centralisé pour stocker les informations d'identification, ce qui permet une authentification unique entre tous les serveurs de la flotte et simplifie l'intercommunication entre les serveurs grâce à l'utilisation de Kerberos pour authentifier les demandes. Avec les objets Stratégie de groupe, vous pouvez gérer les options de configuration de votre flotte. Le déploiement d'un nouveau domaine Active Directory ou l'extension de votre domaine existant au cloud AWS et l'exécution d'instances sur Amazon EC2 offrent de grands avantages. Vous pouvez recourir à l'authentification unique avec Kerberos, exploiter la stratégie de groupe pour gérer la configuration de Windows et administrer aisément les informations d'identification des applications et des utilisateurs à l'aide d'outils Windows natifs tels qu'Utilisateurs et ordinateurs Active Directory.

Certains aspects doivent être pris en compte lors du déploiement d'une forêt Active Directory sur Amazon EC2 : par exemple, comment gérer les instances supplémentaires du contrôleur de domaine, comment appliquer la résolution DNS pour le domaine Active Directory et comment surveiller le trafic de la réplication entre les contrôleurs de domaine des différentes zones de disponibilité. L'une des principales difficultés consiste à joindre les instances Windows Server au domaine Active Directory, parce que vous devez d'abord utiliser la paire de clés Amazon EC2 pour déchiffrer individuellement le mot de passe administrateur de toutes les instances. Ce processus est manuel, gourmand en temps et enclin aux erreurs. Pour les ajouts de serveur à grande échelle, l'étape de la jonction de domaine peut être automatisée. Par exemple, vous pouvez placer un script PowerShell dans l'option User Data afin de joindre l'instance au domaine lors du lancement, mais vous devrez stocker les informations d'identification Active Directory à un emplacement où un script s'exécutant sur une instance nouvellement lancée peut les lire et vous risquez d'exposer des informations d'identification puissantes. Le service AWS Directory et SSM font de la jonction de vos instances à un domaine un processus rapide et à faible risque.

# Présentation d'AWS Directory Service

Il existe deux produits AWS Directory Service : AD Connector et Simple AD. AD Connector vous permet d'utiliser vos identités existantes avec les services AWS sans les répliquer sur AWS. Simple AD vous permet de créer dans AWS un nouvel annuaire compatible avec Active Directory et jouissant d'une profonde intégration aux services AWS. Il n'y a pas de logiciel à installer ; AWS gère les correctifs, les sauvegardes et les mises à niveau, et exécute votre infrastructure d'annuaire entre plusieurs zones de disponibilité à des fins de haute disponibilité.

Après la configuration, vos utilisateurs finaux et administrateurs informatiques peuvent employer leurs informations d'identification professionnelles pour se connecter aux applications AWS, telles qu'Amazon Workspaces, Amazon WorkDocs et Amazon WorkMail, ainsi que pour gérer les ressources AWS telles que les instances Amazon EC2 ou les compartiments Amazon Simple Storage Service (Amazon S3), via l'accès à AWS Management Console basé sur les rôles AWS Identity and Access Management (IAM).

## AD Connector

AD Connector vous permet de connecter un annuaire Active Directory au cloud AWS sans nécessiter une technologie complexe de synchronisation d'annuaire ou entraîner le coût et la complexité liés à l'hébergement d'une infrastructure de fédération. AD Connector est un proxy ; il envoie les demandes aux contrôleurs de domaine de votre domaine, mais ne réplique pas les données de l'annuaire sur AWS. Vos stratégies de sécurité existantes, telles que l'expiration des mots de passe, l'historique des mots de passe et les verrouillages de compte, peuvent être systématiquement mises en œuvre, que les utilisateurs ou les administrateurs informatiques accèdent aux ressources de votre infrastructure sur site ou au cloud AWS.

Vous pouvez également utiliser AD Connector pour activer l'authentification multi-facteurs en l'intégrant à votre infrastructure RADIUS existante. Les utilisateurs bénéficient ainsi d'une sécurité supplémentaire quand ils accèdent aux applications AWS.

Pour plus d'informations, consultez Connexion à votre annuaire avec AD Connector.

## Simple AD

Simple AD est un annuaire Samba géré du cloud AWS. Il prend en charge les fonctionnalités Active Directory couramment utilisées, telles que les comptes d'utilisateur, l'appartenance aux groupes, la jonction de domaine (d'instances Amazon EC2 exécutant Windows Server), l'authentification unique basée sur Kerberos et les stratégies de groupe. La gestion des instances et le déploiement d'applications Windows dans le cloud AWS s'en trouvent encore simplifiés. La plupart de vos applications et outils existants qui requièrent la prise en charge d'Active Directory peuvent être utilisés avec Simple AD. Par défaut, Simple AD fournit des instantanés quotidiens et automatisés afin de permettre la récupération à un instant donné.

Pour plus d'informations, consultez Création d'un annuaire avec Simple AD.

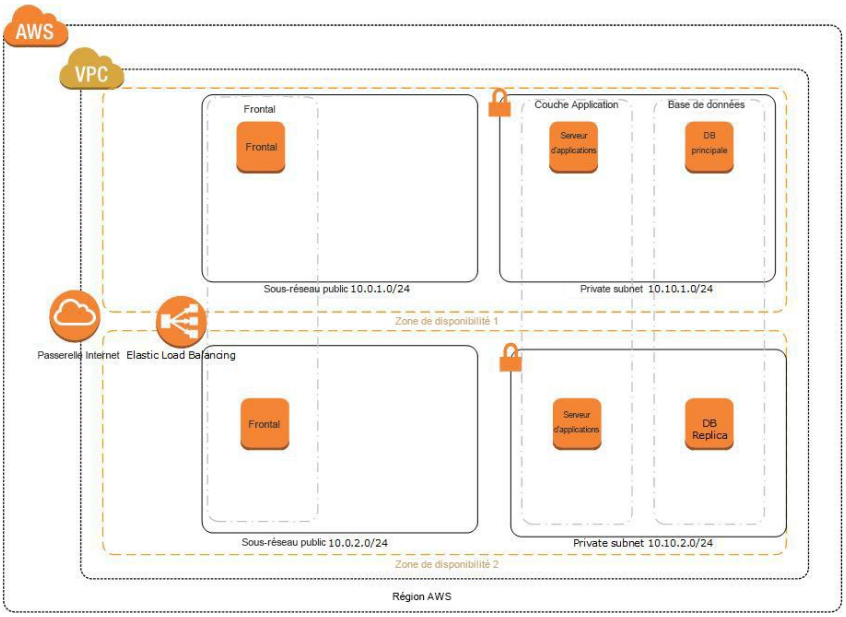
# Joindre les instances Amazon EC2 pour Windows à un domaine AWS

SSM vous permet de configurer, gérer et déployer les configurations serveur sur les instances Amazon EC2 exécutant les charges de travail et les applications Windows Server. La fonctionnalité SSM de jonction de domaine réduit le nombre d'étapes requises pour joindre les instances Amazon EC2 exécutant Windows Server sur un annuaire Simple AD lors du lancement. Vous pouvez utiliser SSM pour créer un document de configuration JSON avec les tâches de configuration, puis associer le document à une ou plusieurs instances Windows. Le service EC2Config est installé sur les AMI AWS Windows. Lorsque vous lancez une nouvelle instance Amazon EC2 exécutant Windows, le service EC2Config appelle SSM pour obtenir et appliquer les configurations associées à votre instance. Le service EC2Config vérifie aussi régulièrement les mises à jour de configuration à appliquer. SSM peut être utilisé pour automatiser l'installation ou la suppression de packages MSI, exécuter les scripts PowerShell, configurer et exporter les données du journal des événements Windows Server vers les journaux Amazon CloudWatch. L'extension SSM nécessite EC2Config 3.0 ou version ultérieure. Si vous n'avez pas lancé votre instance depuis un AMI Windows actif, vous pouvez installer la dernière version d'EC2Config en suivant les étapes décrites ici.

La jonction de domaine met à profit SSM et AWS Management Console pour créer un document de configuration JSON que SSM utilise pour joindre de façon transparente les instances Windows Server aux domaines AWS Directory Service. Vous supprimez aussi la nécessité de vous connecter à chaque instance Amazon EC2 exécutant Windows avant de la joindre au domaine AWS Directory Service ou de vous exposer au risque de placer les informations d'identification du domaine dans un script PowerShell.

# Exemple Amazon EC2 pour Windows

La figure suivante illustre l'architecture traditionnelle d'une application Windows : un VPC avec quatre sous-réseaux (deux privés et deux publics) répartis entre deux zones de disponibilité. Les couches application et base de données se trouvent dans les sous-réseaux privés ; les serveurs web frontaux se trouvent dans les sous-réseaux publics.




**Figue 1 : VPC avec quatre sous-réseaux**

SQL Server s'exécute dans la couche base de données. L'authentification Kerberos est requise pour permettre l'utilisation d'un outil d'aide à la décision. Vous devez vous assurer que les instances sont configurées pour répondre aux exigences de sécurité de votre entreprise, lesquelles nécessitent IPsec pour sécuriser la communication entre les serveurs d'application et de base de données, ainsi que BitLocker pour chiffrer les volumes de données des serveurs de base de données. Pour satisfaire ces exigences, vous créez un objet Stratégie de groupe avec les paramètres et la gestion de groupe locale appropriés pour accorder les autorisations au groupe Active Directory Administrateurs DBA.

Avec l'objet Stratégie de groupe créé et stocké dans AWS Directory Service, voici quelques étapes pour vous assurer que les instances Windows nouvelles et existantes lancées dans le sous-réseau privé répondent à vos exigences :

1. Utilisez les filtres Windows Management Instrumentation (WMI) pour configurer les objets Stratégie de groupe et les appliquer aux instances exécutant Windows.
2. Joignez de façon transparente ces instances au domaine AWS Directory Service.
3. Vérifiez que les instances sont configurées correctement.

## Utiliser les filtres WMI pour appliquer les objets Stratégie de groupe

La possibilité d'automatiser l'ajout et la suppression de serveurs sur vos instances Amazon EC2 peut rendre difficile l'application cohérente des paramètres de configuration.

Même s'il existe de nombreux outils pour détecter dynamiquement l'ajout de nouveaux serveurs (par exemple, System Center Configuration Manager), le présent livre blanc se concentre sur les outils et méthodes fournis avec Windows Server, principalement les objets Stratégie de groupe.

WMI est l'infrastructure de gestion des données et des opérations sur les systèmes d'exploitation Windows. Vous pouvez écrire des applications ou des scripts WMI pour automatiser les tâches administratives sur les ordinateurs distants, mais WMI fournit aussi les données de gestion aux autres parties du système d'exploitation et aux produits tels que System Center Operations Manager et Windows Remote Management (WinRM).

Les filtres WMI vous permettent de déterminer dynamiquement l'étendue des objets Stratégie de groupe en fonction des attributs de l'ordinateur cible. Quand un objet Stratégie de groupe lié à un filtre WMI est appliqué sur l'ordinateur cible, le filtre est évalué sur ce dernier. Si le filtre WMI a la valeur false, l'objet Stratégie de groupe n'est pas appliqué. Si le filtre WMI a la valeur true, l'objet Stratégie de groupe est appliqué. Avec les filtres WMI, l'objet Stratégie de groupe est appliqué sur les nouvelles instances lancées dynamiquement en fonction des informations relatives à l'instance (le sous-réseau de l'instance, par exemple).

Avec les filtres WMI, vous pouvez vous assurer que les objets Stratégie de groupe liés au domaine AWS Directory Service sont appliqués en fonction du sous-réseau dans lequel vous avez lancé l'instance. Dans l'exemple d'architecture illustré à la figure 1, le sous-réseau privé de la zone de disponibilité 1 est 10.10.1.0/24. Avec le filtre WMI suivant, les objets Stratégie de groupe ne sont appliqués qu'aux instances lancées dans le sous-réseau privé de la zone de disponibilité 1 :

```
Select * FROM Win32_IP4RouteTable
 WHERE ((Mask='255.255.255.255' AND NextHop='0.0.0.0')
 AND (Destination Like '10.10.1.255'))
```

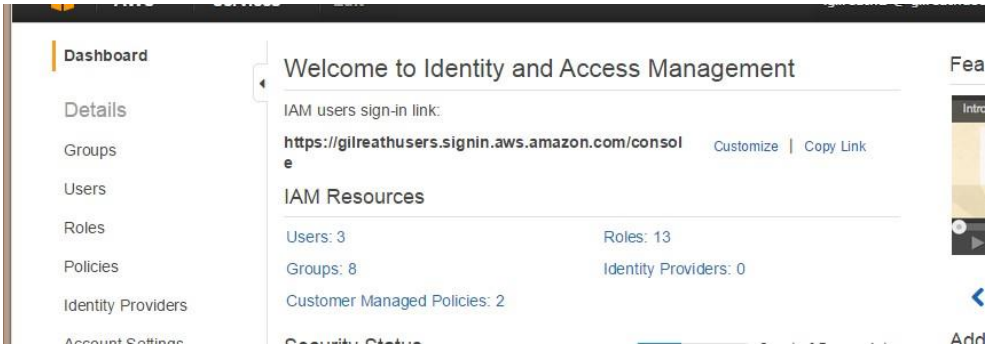
Pour déterminer le sous-réseau de l'instance, le filtre WMI examine la table de routage, recherche l'itinéraire avec un masque de sous-réseau 32 bits, un tronçon suivant de valeur 0.0.0.0 (qui indique l'adresse IP de l'instance) et une destination qui corresponde au sous-réseau souhaité.

Au fur et à mesure que de nouvelles instances sont lancées manuellement ou via une automatisation telle qu'Auto Scaling, le filtre WMI est évalué. Si l'instance est lancée dans le sous-réseau 10.10.1.0/24, l'objet Stratégie de groupe est appliqué.

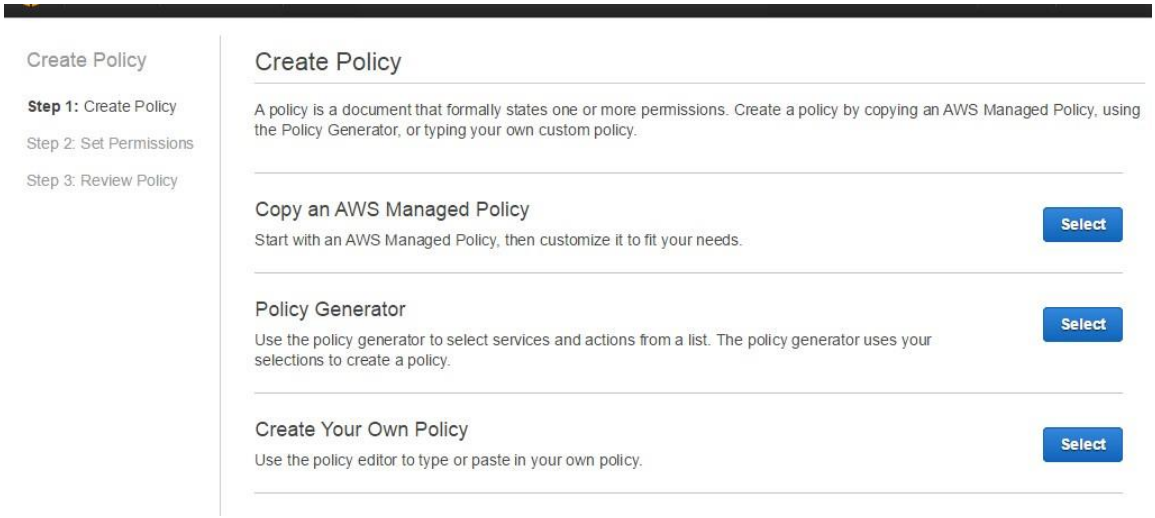
## Joindre les instances au domaine AWS Directory Service

Après que vous avez utilisé Simple AD ou AD Connector pour définir un domaine dans AWS Directory Service, vous pouvez configurer les instances Windows de façon à joindre le domaine au lancement. Comme les instances Windows doivent pouvoir appeler l'API SSM, placez-les dans un rôle avec accès à l'API SSM Amazon EC2. Un rôle est essentiellement un ensemble d'autorisations qui accordent l'accès aux actions et aux ressources d'AWS. Ces autorisations sont attachées au rôle, et non pas à un utilisateur ou un groupe IAM. Vous définissez les autorisations d'un rôle dans une stratégie IAM, laquelle est un document JSON écrit dans la langue de la stratégie IAM. Lorsque vous créez le rôle, vous créez deux stratégies distinctes pour celui-ci : la stratégie d'approbation, qui spécifie les personnes autorisées à assumer le rôle (l'entité autorisée, ou mandataire), et la stratégie d'autorisation, qui définit les actions et les ressources que le mandataire peut utiliser. Les rôles peuvent être utilisés par un service AWS, tel qu'Amazon EC2. Un rôle est attribué à une instance Amazon EC2 lors du lancement ; il ne peut pas être assigné à une instance qui est déjà en cours d'exécution. Pour plus d'informations, consultez Utilisation de rôles IAM pour déléguer les autorisations aux applications qui s'exécutent sur Amazon EC2.

Vous devez d'abord créer la stratégie à attacher à un rôle. Dans le volet de navigation d'AWS Management Console, cliquez sur **Policies**.




Choisissez **Create Policy**, puis **Select** pour créer votre propre stratégie.




Entrez le nom et la description de votre stratégie, collez le texte suivant dans le document de stratégie, puis choisissez **Create Policy**.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid":
            "AllowaccesstoSSM",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:ListAssociations",
                "ssm:GetDocument",
                "ssm:UpdateAssociationStatus",
                "ds:CreateComputer",
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Les détails du document de stratégie vous aideront à comprendre les autorisations attribuées par la stratégie :

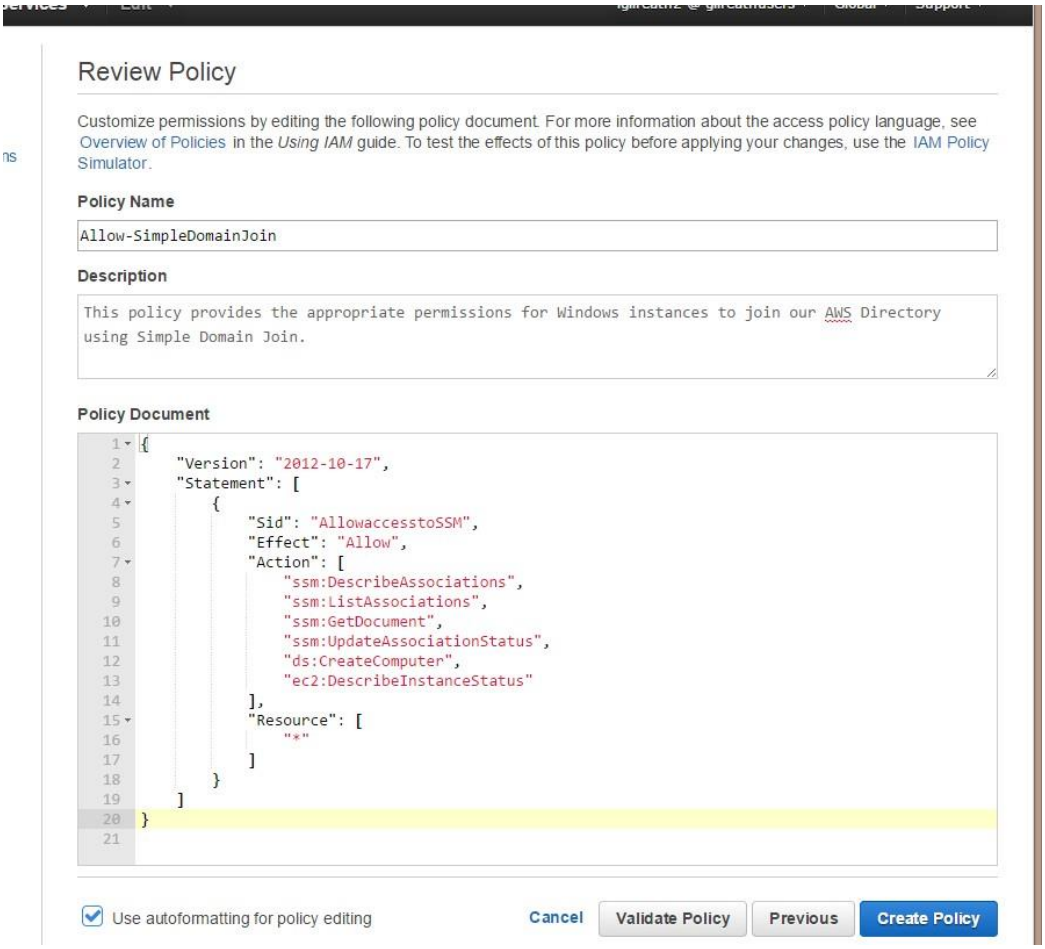
**ssm:DescribeAssociation** : appel d'API qui décrit les associations du document de configuration ou de l'instance spécifié.

**ssm:ListAssociations** : répertorie les associations du document de configuration ou de l'instance spécifié.

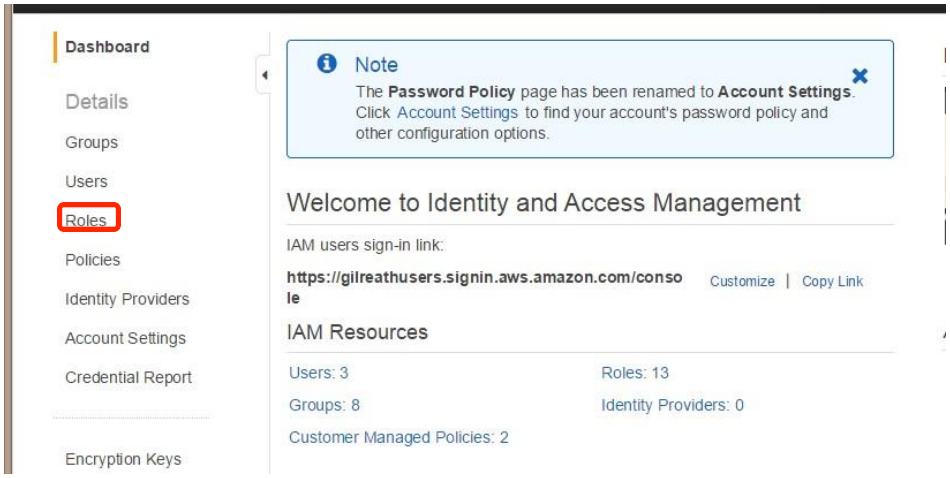
**ssm:GetDocument** : obtient le contenu du document de configuration spécifié.

**ssm:UpdateAssociationStatus** : met à jour le statut du document de configuration associé à l'instance spécifiée.

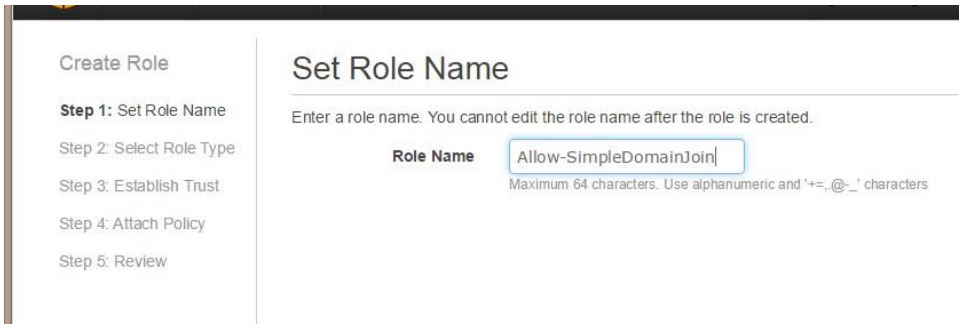
**ds:CreateComputer** : permet la création d'un objet ordinateur dans le domaine AWS Directory Service.



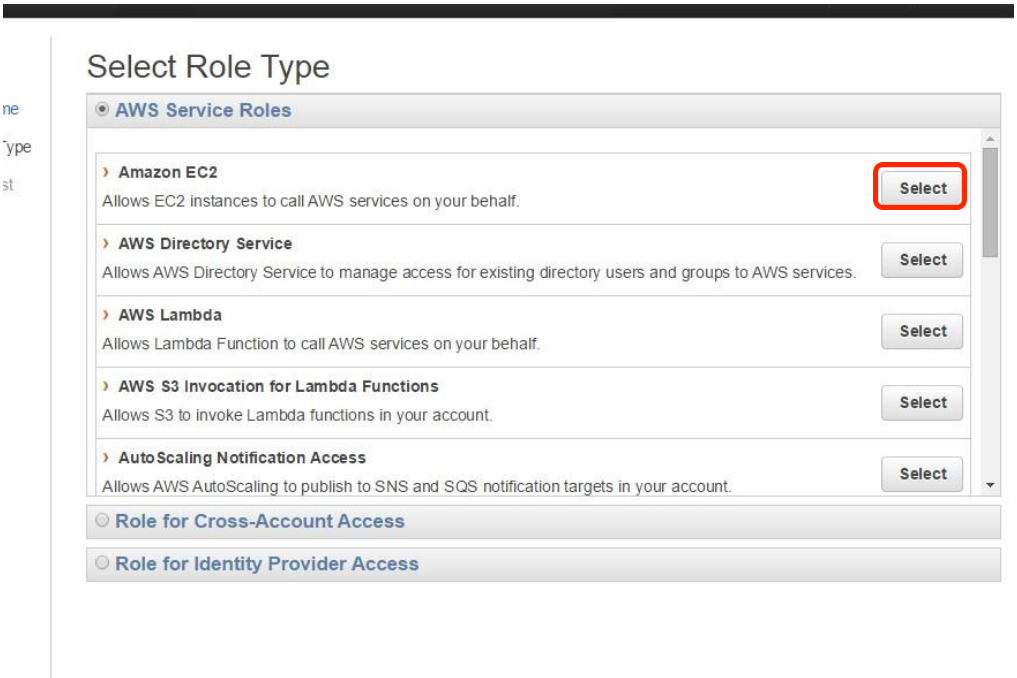

Dans le volet de navigation, sous **Dashboard**, choisissez **Roles**.



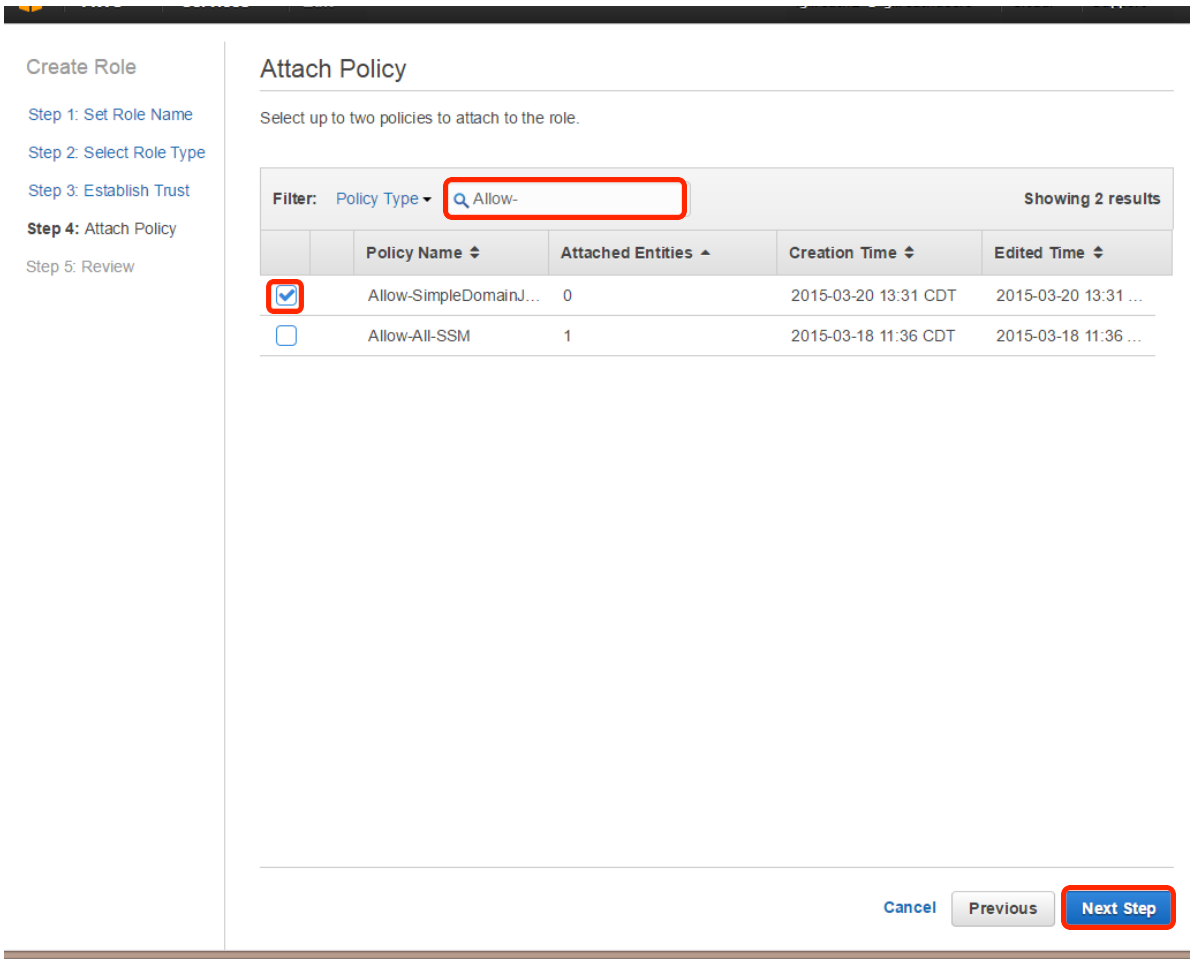

Choisissez **Create Role,** entrez un nom pour votre rôle, puis choisissez **Next Step**.




Dans la page **Select Role Type** , sélectionnez **Amazon EC2**.




Sur la page **Attach Policy**, recherchez la stratégie que vous avez créée à l'étape précédente, sélectionnez-la, puis choisissez **Next Step**.

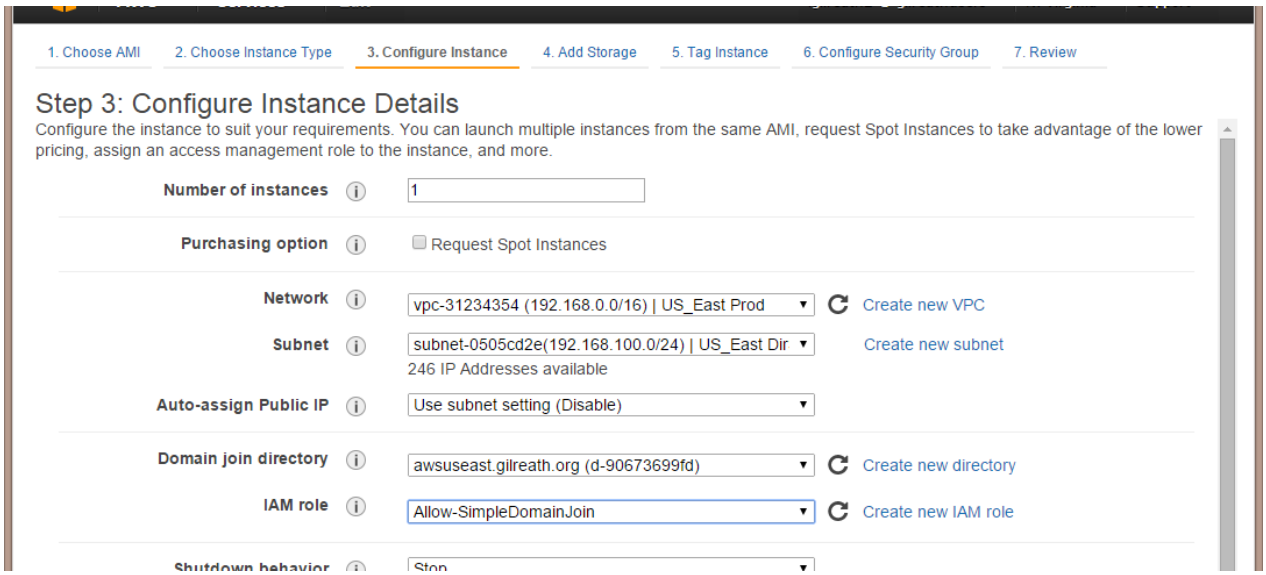



Dans la page **Review** , choisissez **Create Role**.

Vous pouvez utiliser l'option de l'Assistant **Launch More Like This** dans la console Amazon EC2 pour joindre de façon transparente une nouvelle instance à un domaine que vous spécifiez.

### Pour joindre un domaine à l'aide de l'Assistant

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.Amazon.com/.
2. Dans la console Amazon EC2, cliquez sur **Launch Instance**.
3. Dans la première page de l'Assistant, sélectionnez un AMI Windows, puis cliquez sur **Next**. Sur la page suivante, sélectionnez un type d'instance, puis cliquez sur **Next**.
4. Dans la liste déroulante **Network** , sélectionnez un VPC. Veillez à sélectionner un VPC situé dans votre domaine AWS Directory Service. Dans la liste déroulante **Subnet** , sélectionnez un sous-réseau.



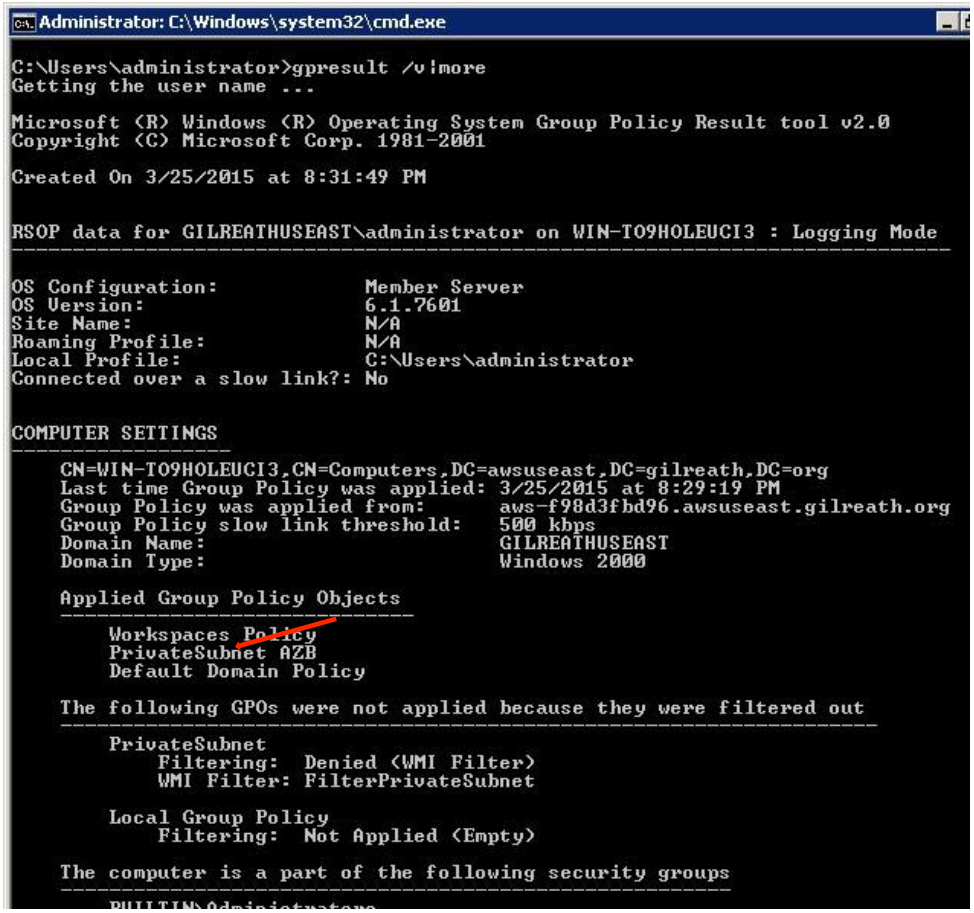

5. Dans la liste déroulante **Domain join directory** , sélectionnez votre domaine. Dans la liste déroulante **IAM role** , sélectionnez le rôle IAM à associer à l'instance.
6. Complétez le reste des étapes de configuration comme requis, puis cliquez sur **Next**.
7. Lorsque vous atteignez l'étape 6 de l'Assistant, assurez-vous de sélectionner ou de créer un groupe de sécurité avec une règle autorisant l'accès RDP depuis votre adresse IP, ou depuis une plage d'adresses IP, au sein de votre réseau. Pour plus d'informations sur les règles de groupe de sécurité, consultez Autorisation du trafic entrant pour vos instances Windows.
8. Cliquez sur **Review and Launch** pour lancer votre instance.
9. Vérifiez l'état de la jonction du domaine. Pour plus d'informations, consultez Obtention du statut de la jonction de domaine.

## Vérifier que les instances sont configurées correctement

Après que l'instance a été lancée et jointe au domaine avec succès, vous pouvez vous connecter à votre instance à l'aide des informations d'identification du domaine que vous avez définies dans AWS Directory Service. Suivez les étapes ci-après pour vous connecter à votre instance Windows à l'aide de RDP.

A partir d'une ligne de commande sur l'instance Windows, exécutez gpupdate /force pour actualiser les paramètres de Stratégie de groupe sur l'instance.


Exécutez gpresult /v pour afficher les résultats.




Dans la section Applied Group Policy Objects, vous pouvez voir votre objet Stratégie de groupe. S'il n'apparaît pas, consultez les journaux des événements ou suivez ces recommandations de dépannage.

# Conclusion

AWS Directory Service et la fonction de jonction de domaine dans SSM rendent plus simple la gestion de votre flotte Windows sur Amazon EC2. AWS Directory Service vous épargne d'avoir à gérer un domaine distinct et des contrôleurs de domaine, pour une partie du coût de l'exécution de plusieurs contrôleurs de domaine gérés automatiquement sur Amazon EC2. La fonction de jonction de domaine de SSM fait de l'ajout d'instances Windows à un domaine AWS Directory Service un processus qui peut être inclus dans l'automatisation. De plus, la possibilité d'utiliser des outils natifs pour Windows autorise les options de gestion et de configuration qui reflètent vos normes locales. L'exécution de Windows sur Amazon EC2 a toujours fourni une flexibilité avec une sécurité bien définie. Avec AWS Directory Service et la fonction de jonction de domaine dans SSM, AWS continue d'être le meilleur emplacement pour exécuter les charges de travail Windows.