Déploiement sur AWS

- Déploiement sur AWS, à la page 1
- Préparation de votre environnement, à la page 3
- Sélection de l'AMI de l'appliance virtuelle et sélection du type d'instance, à la page 4
- Configurer les détails de l'instance, à la page 7
- Configuration du stockage et ajout de balises, à la page 8
- Configuration du groupe de sécurité, vérification et lancement de l'instance, à la page 8
- Configurer l'instance lancée, à la page 9
- Connexion à l'interface Web de l'appliance, à la page 9
- Création d'adresses IP élastiques, à la page 10
- Configurer l'appliance afin qu'elle envoie des alertes à l'approche de l'expiration de la licence, à la page 11

Déploiement sur AWS

Remarque

- Les appliances sur site Cisco Secure Email Gateway ne sont pas prises en charge sur les déploiements de l'appliance Cisco Secure Email and Web Manager sur AWS.

Effectuez les étapes suivantes pour déployer une appliance virtuelle Secure Email Gateway, Secure Web ou Secure Email and Web Manager :

	Faire ceci	Plus d'informations
Étape 1	Préparez votre environnement en effectuant les tâches prérequises et en acquérant les informations dont vous aurez besoin avant de configurer une instance dans EC2.	Préparation de votre environnement

Déploiement sur AWS

	Faire ceci	Plus d'informations
Étape 2	Sélectionner l'AMI sur la Place de marché Amazon et sélectionner le type d'instance approprié. **Remarque** Secure Email Gateway n'est pas disponible sur la Place de marché AWS; communiquez avec votre représentant commercial Cisco en lui donnant les détails de votre compte AWS (nom d'utilisateur et région) pour provisionner une AMI.	Sélection de l'AMI de l'appliance virtuelle et sélection du type d'instance.
Étape 3	Configurez le réseau, le sous-réseau, l'attribution de l'adresse IP et les autres détails nécessaires pour que votre instance soit disponible et fonctionne comme prévu. **Remarque** Une interface réseau principale (gestion) est automatiquement attribuée à une instance. Au besoin, vous pouvez créer des interfaces de données (P1, pour S100V; P1, P2 pour S300V et S600V).	Configurer les détails de l'instance
Étape 4	Conservez les paramètres de stockage par défaut ou configurez les balises selon les besoins.	Configuration du stockage et ajout de balises.
Étape 5	Configurez le groupe de sécurité. Passez en revue tous les paramètres de configuration et lancez l'instance.	Configuration du groupe de sécurité, vérification et lancement de l'instance.
Étape 6	Installez la licence dans l'appliance et empêchez l'interface Web de répondre avec le nom d'hôte propre à l'appliance. Utilisez la commande **hostheader** et validez la modification.	Configurer l'instance lancée.
Étape 7	Connectez-vous à l'interface Web de l'appliance. Vous pouvez exécuter l'assistant de configuration du système, téléverser un fichier de configuration ou configurer les fonctionnalités.	Connexion à l'interface Web de l'appliance.
Étape 8	(Facultatif) Si nécessaire, configurez les adresses IP élastiques dans la console de gestion AWS EC2.	Création d'adresses IP élastiques.
Étape 9	Configurez l'appliance pour qu'elle envoie des alertes d'expiration de licence.	Configurer l'appliance afin qu'elle envoie des alertes à l'approche de l'expiration de la licence.

Préparation de votre environnement

Assurez-vous de disposer des ressources et des fichiers nécessaires pour déployer les appliances virtuelles Secure Email Gateway, Secure Web ou Secure Email and Web Manager sur AWS EC2. Notamment :

- Une licence valide pour les appliances virtuelles Secure Email Gateway, Secure Web ou Secure Email and Web Manager.
- Le nom d'utilisateur et le mot de passe par défaut de votre appliance pour la sécurité Web :

  – `admin` et `ironport`
- Ressources de votre console de gestion EC2 :

  – Si vous avez besoin d'une adresse IP publique de nœud persistant qui peut être associée aux instances, décidez de l'adresse IP élastique à utiliser ou créez-en une nouvelle. L'adresse IP publique qui est automatiquement attribuée lors du processus de lancement d'une nouvelle instance est dynamique.

  – Assurez-vous de savoir quel VPC vous allez utiliser ou configurez un VPC qui sera utilisé avec le déploiement. Vous pouvez également utiliser le VPC par défaut.

  – En fonction de la façon dont les administrateurs et les autres utilisateurs accéderont à l'appliance, vous devez déterminer le type d'adresse IP à attribuer à l'appliance (publique ou privée).

  – Sachez quel rôle IAM utiliser ou configurez un rôle IAM à utiliser avec le déploiement.

  – Configurez le sous-réseau et vérifiez que la table de routage contient la voie de routage par défaut orientée vers la passerelle Internet.

  – Configurez le groupe de sécurité, ou créez-en un nouveau.

  – Les ports les plus courants à ouvrir pour que l'appliance virtuelle communique correctement sont les suivants :

    - SSH TCP 22
    - TCP 443
    - TCP 8443
    - TCP 3128
    - (Facultatif) ICMP, si nécessaire, pour le débogage.
- Confirmez que vous pouvez accéder à la clé privée (fichier PEM ou CER) que vous souhaitez qu'AWS enregistre avec l'instance EC2. Vous pouvez également créer une nouvelle clé privée pendant le processus de lancement de l'instance de l'appliance virtuelle.

Remarque Pour les clients Windows, vous aurez besoin d'un client SSH pour accéder au fichier PEM.

Sélection de l'AMI de l'appliance virtuelle et sélection du type d'instance

Assurez-vous que la bonne région est sélectionnée dans votre compte AWS.

Étape 1 Accédez à votre console de gestion EC2.

Étape 2 Cliquez sur **Launch Instance** (Lancer l'instance) et sélectionnez **Launch Instance** (Lancer l'instance) dans la liste déroulante.

Étape 3 Cliquez sur **AWS Marketplace** (Place de marché AWS).

Remarque Secure Email Gateway n'est pas disponible sur la Place de marché AWS; communiquez avec votre représentant commercial Cisco en lui donnant les détails de votre compte AWS (nom d'utilisateur et région) pour provisionner une AMI.

Étape 4 Sélectionnez le type d'instance en fonction du modèle de l'appliance virtuelle. Par exemple, si vous avez besoin du modèle S300V d'appliance virtuelle Cisco Secure Web, sélectionnez c4.xlarge ainsi que le vCPU, la vRAM, etc. correspondants.

Produit	Version d'AsyncOS	Modèle	Type d'instance EC2	Processeur virtuel	vRAM	vNIC	Taille minimale du disque
Appliance virtuelle Cisco Secure Email Gateway	AsyncOS 14.0 ou versions ultérieures (courriel)	**C100V**	c4.xlarge	4	7,5 Go	1 (*)	200 Go
		C300V	c4.2xlarge	8	15 Go	1 (*)	500 Go
		C600V	c4.4xlarge	16	30 Go	1 (*)	500 Go

(*) Une seule carte réseau est présentée par défaut, mais l'utilisateur peut créer une interface supplémentaire lors du lancement de l'instance.

Produit	Version d'AsyncOS	Modèle	Type d'instance EC2	Processeur virtuel	vRAM	vNIC	Taille minimale du disque
Appliance virtuelle Cisco Secure Web	AsyncOS 14.5 ou versions ultérieures (Web)	**S100V**	c5.xlarge	4	8 Go	2	200 Go
		S300V	c5.2xlarge	8	16 Go	3	500 Go
		S600V	c5.4xlarge	16	32 Go	3	750 Go
	AsyncOS 14.0 ou versions ultérieures (Web)	**S100V**	m4.large	2	8 Go	2	200 Go
		S300V	c4.xlarge	4	7,5 Go	3	500 Go
		S600V	c4.4xlarge	16	30 Go	3	750 Go

Produit	Version d'AsyncOS	Modèle	Type d'instance EC2	Processeur virtuel	vRAM	Taille minimale du disque
Appliance virtuelle Cisco Secure Email and Web Manager	AsyncOS 14.0 ou versions ultérieures	**M100V**	Actuellement, l'image n'est pas disponible.	-	-	-
		M300V	c4.xlarge	4	7,5 Go	1 024 Go
		M600V	c4.2xlarge	8	15 Go	2 032 Go

Remarque
- Lorsque vous configurez une appliance C100V et S300V avec 7,5 Go de vRAM, vous verrez des messages d'avertissement concernant une image de machine virtuelle mal configurée ou un état RAID sous-optimal. Ces messages d'avertissement s'affichent lors de l'utilisation des commandes de la CLI comme **Loadlicense** (Charger une licence) et **Upgrade** (Mettre à niveau). Vous pouvez ignorer ces messages en toute sécurité. La configuration de la vRAM n'aura aucune incidence sur le fonctionnement normal de l'appliance.
- Si vous utilisez le routage fractionné sur l'appliance virtuelle Secure Web, vous devez attribuer une adresse IP publique (IP élastique) au port d'écoute du proxy.

Étape 5 Cliquez ensuite sur **Configure Instance Details** (Configurer les détails de l'instance).

Déploiement de Secure Web Appliance (SWA) sur AWS pour Coeus 14.5

Pour une analyse d'AWS réussie pour Coeus 14.5, procédez comme suit :

Étape 1 Déployez une AMI avec les type d'instances **C4** correspondants, comme indiqué dans le tableau suivant :

Modèle	Type d'instance
S100V	m4.large
S300V	c4.2xlarge
S600V	c4.4xlarge

Étape 2 Lorsqu'une instance est active, vérifiez son accessibilité en vous y connectant à l'aide de **SSH** et des informations d'authentification de l'administrateur.

Étape 3 Arrêtez l'instance à l'aide de la CLI de Secure Web Appliance et vérifiez-la à l'aide de la CLI d'AWS.

Étape 4 Pour mettre à jour les instances, connectez la CLI d'AWS avec l'identifiant de la clé d'accès et la clé d'accès secrète.

Étape 5 Pour vérifier si l'ENA est déjà activé dans l'instance EC2, exécutez la commande suivante avec l'identifiant de l'instance et la région.

```
aws ec2 describe-instances --instance-id <your-instance-id>
--query"Reservations[].Instances[].EnaSupport" --region <your-region>
```

- Si l'ENA est activé avec succès, il renvoie l'état **« True »** (Vrai). Passez à l'Étape 7.

- Si l'ENA n'est pas activé, il renvoie une chaîne vide. Passez à l'étape suivante.

Étape 6 Pour activer l'ENA dans une instance EC2, exécutez la commande suivante :

```
aws ec2 modify-instance-attribute --instance-id <your-instance-id> --ena-support --region
<your-region>
```

Remarque Cette commande ne renvoie aucune information. Passez à l'Étape 5.

Étape 7 Modifiez le type d'instance **C4** pour **C5**, comme indiqué dans le tableau suivant :

Modèle	Type d'instance
S100V	c5.xlarge
S300V	c5.2xlarge
S600V	c5.4xlarge

Étape 8 Démarrez l'instance.

Prochaine étape

Remarque La mise à niveau des instances d'AWS de coeus 14.0 vers coeus 14.5 n'est pas prise en charge. Nous vous recommandons de déployer la nouvelle instance dans coeus 14.5.

Si vous avez une instance d'AWS en cours d'exécution dans coeus 14.0 et souhaitez créer une configuration compatible pour charger l'instance coeus 14.5 nouvellement déployée, mettez à niveau l'instance coeus 14.0 vers coeus 14.5. Vous pourrez ensuite télécharger la configuration. Pour en savoir plus, consultez la section Saving, Loading, and Resetting the Appliance Configuration (Enregistrement, chargement et réinitialisation de la configuration de l'appliance) du Guide d'utilisation de Secure Web Appliance (recommandé uniquement pour obtenir une configuration compatible avec coeus 14.5).

Pour connaître la procédure de chargement de la configuration compatible dans la nouvelle instance coeus 14.5 déployée, consultez la section Loading the Appliance Configuration File (Chargement du fichier de configuration de l'appliance) du Guide d'utilisation de Secure Web Appliance.

Pour en savoir plus :

- L'installation et la configuration de la CLI d'AWS, consultez

  https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html.

- Pour le programme d'installation et la configuration des prérequis pour l'utilisation de l'AWS CLI, consultez

  https://docs.aws.amazon.com/cli/latest/userguide/getting-started-prereqs.html.

Configurer les détails de l'instance

Étape 1 Saisissez le nombre d'instances.

Remarque L'option d'achat d'instances ponctuelles vous permet d'acheter de la capacité de calcul supplémentaire dans le nuage d'AWS. Pour en savoir plus, consultez la documentation d'Amazon EC2.

Étape 2 Sélectionnez le bon VPC dans la liste déroulante **Network** (réseau).

Étape 3 Sélectionnez le sous-réseau requis pour ce déploiement dans la liste déroulante **Subnet** (sous-réseau).

Étape 4 Sélectionnez l'option requise dans la liste déroulante **Auto-assign Public IP** (Attribuer automatiquement une adresse IP publique) :

— Sélectionnez **Use subnet settings (Enable)** (Utiliser les paramètres du sous-réseau [Activer]) pour attribuer une adresse IP publique en fonction des paramètres définis dans les paramètres de sous-réseau.

— Sélectionnez **Enable** (Activer) pour demander une adresse IP publique pour cette instance. Cette option remplace les paramètres de sous-réseau pour les adresses IP publiques.

– Sélectionnez **Disable** (Désactiver) si vous n'avez pas besoin d'une adresse IP publique attribuée automatiquement. Cette option remplace les paramètres de sous-réseau pour les adresses IP publiques.

Étape 5 Sélectionnez le rôle IAM.

Étape 6 Sélectionnez le **Shutdown behavior** (Comportement à l'arrêt). Cisco vous recommande de sélectionner **Stop** (Arrêter).

Mise en garde Sélectionner **Terminate** (Résilier) supprimera l'instance et toutes ses données.

Étape 7 (Facultatif) Cochez la case **Protect against accidental termination** (Protéger contre la résiliation accidentelle).

Étape 8 (Facultatif) Passez en revue et sélectionnez d'autres options comme **Monitoring** (Surveillance), **EBS-optimized instance** (Instance optimisée pour EBS) et **Tenancy** (Location), selon vos besoins.

Étape 9 Sélectionnez la **Network Interface** (Interface réseau).

- Vous pouvez ajouter d'autres interfaces au besoin à partir d'interfaces réseau créées précédemment.
- Pour ajouter une autre interface réseau, sélectionnez **Add Device** (Ajouter un périphérique). Vous pouvez spécifier jusqu'à deux interfaces réseau lorsque vous lancez une instance. Après avoir lancé l'instance, sélectionnez **Network Interfaces** (Interfaces réseau) dans le volet de navigation pour ajouter des interfaces réseau supplémentaires.
- Vous ne pouvez pas attribuer automatiquement une adresse IP publique si vous spécifiez plus d'une interface réseau.
- Il y a un nombre maximal d'interfaces réseau que vous pouvez créer pour un type d'instance. Voir l'étape 4 de la section Sélection de l'AMI de l'appliance virtuelle et sélection du type d'instance.
- Voir la section Création d'adresses IP élastiques pour créer des adresses IP statiques.

Configuration du stockage et ajout de balises

Étape 1 Conservez les options de stockage par défaut. Vous pouvez les modifier au besoin.

Remarque Cisco recommande d'utiliser les disques SSD d'IOPS provisionnées pour tous les déploiements. Vous pouvez utiliser un disque SSD à usage général, mais le disque SSD IOPS provisionné offre des performances optimales. Il peut s'écouler jusqu'à 45 minutes pour que votre instance soit disponible pour la première connexion.

Étape 2 Saisissez les balises requises. Vous pouvez créer une balise ou plusieurs balises pour une instance.

Par exemple, *name* (nom) comme la clé et sa valeur, *Cisco wsa*.

Configuration du groupe de sécurité, vérification et lancement de l'instance

Étape 1 Sélectionnez le **groupe de sécurité** approprié pour le déploiement.

Étape 2 Cliquez sur **Review and Launch** (Vérifier et lancer).

Étape 3 Vérifiez votre configuration et assurez-vous que tous les détails correspondent à vos besoins.

Étape 4 Lancez l'instance.

Étape 5 Sélectionnez une paire de clés existante ou créez-en une nouvelle et téléchargez-la. La création d'une instance sans paire de clés n'est pas possible.

Étape 6 Cliquez sur **Launch** (Lancer) pour lancer l'instance.

Étape 7 Cliquez sur **Instances**.

Vous serez en mesure de visualiser la nouvelle instance configurée sur la page EC2 **Instances**. Si les vérifications de l'instance sont réussies, une coche verte s'affiche dans la colonne **Status Checks** (vérifications de l'état), suivie de la mention **2/2checks passed** (2/2 vérifications réussies).

Étape 8 (Facultatif) Affichez le journal du système en procédant comme suit :

1. Sur la page **Instances**, sélectionnez l'instance.
2. Cliquez sur **Actions**.
3. Cliquez sur **Get System Log** (Obtenir le journal système) sous **Instance Settings** (Paramètres de l'instance).
4. Si une invite de connexion s'affiche, cela indique que l'instance est opérationnelle et en cours d'exécution.

Étape 9 (Facultatif) Si vous avez choisi d'attribuer une adresse IP publique à l'instance, vérifiez si vous y accédez en utilisant l'adresse IP publique.

Configurer l'instance lancée

Remarque Sur Secure Web Appliance, l'accès SSH pour l'utilisateur « admin » par défaut fonctionne uniquement avec l'authentification par clé. L'authentification par mot de passe sera disponible pour les utilisateurs qui sont configurés à l'aide de la commande CLI **userconfig** et de l'interface graphique utilisateur de l'application sous **System Administration (Administration système)** > **Users (Utilisateurs)**.

Étape 1 Cliquez sur **Instances** dans votre panneau de navigation EC2.

Étape 2 Sélectionnez l'instance et cliquez sur **Connect** (Connecter).

Étape 3 Passez en revue les informations de connectivité dans la boîte de dialogue **Connect to Your Instance** (Connectez-vous à votre instance). Vous aurez besoin de ces informations pour vous connecter à l'appliance virtuelle via SSH. Cela inclut le fichier PEM utilisé avec le DNS public. Assurez-vous que votre clé n'est pas visible publiquement.

Remarque Le nom d'utilisateur par défaut est `admin`, et non « root » comme indiqué.

Étape 4 Utilisez un client SSH pour vous connecter à l'instance.

Étape 5 Utilisez la commande **Loadlicense** (Charger une licence) pour coller la licence via la CLI ou la charger à partir d'un fichier.

Remarque Pour les appliances C100V et S300V avec la vRAM de 7,5 Go recommandée, vous verrez des messages d'avertissement concernant une image de machine virtuelle mal configurée ou un état RAID sous-optimal. Ces messages d'avertissement s'affichent lors de l'utilisation des commandes de la CLI comme **Loadlicense** (Charger une licence) et **Upgrade** (Mettre à niveau). Vous pouvez ignorer ces messages en toute sécurité. La configuration de la vRAM n'aura aucune incidence sur le fonctionnement normal de l'appliance.

Étape 6 Empêchez l'interface Web de répondre avec le nom d'hôte propre à l'appliance. Utilisez la CLI **adminaccessconfig** > **hostheader** et validez la modification.

Consultez la section « Additional Security Settings for Accessing the Appliance » (Paramètres de sécurité supplémentaires pour l'accès à l'appliance) du chapitre « Perform System Administration Tasks » (Effectuer des tâches d'administration système) du guide d'utilisation Cisco Secure Web Appliance.

Connexion à l'interface Web de l'appliance

Utilisez l'interface Web pour configurer le logiciel de l'appliance. Lorsque vous sélectionnez une instance, son adresse IP s'affiche dans l'onglet **Description**. Le nom d'utilisateur et le mot de passe par défaut sont **admin** et **ironport**.

Le tableau suivant répertorie les ports par défaut pour les appliances virtuelles :

Produit	Port HTTP	Port HTTPS
Cisco Secure Web Appliance	8080	8443

Produit	Port HTTP	Port HTTPS
Cisco Secure Email Gateway	80	443
Cisco Secure Email and Web Manager	80	443

Par exemple, vous pouvez :

- Exécuter l'assistant de configuration du système

Remarque L'adresse IP et la passerelle par défaut proviennent d'AWS. Ces dernières peuvent être conservées. Une bonne pratique consiste à bloquer tous les programmes malveillants.

- Téléverser un fichier de configuration.
- Configurer manuellement les caractéristiques et les fonctionnalités.
- Pour obtenir des instructions sur l'accès à l'appliance et sa configuration, y compris la collecte des informations nécessaires, consultez l'aide en ligne ou le guide d'utilisation de votre version d'AsyncOS, disponible à l'emplacement approprié dans Additional Information.
- Pour migrer les paramètres d'une appliance physique, consultez les notes de mise à jour pour votre version d'AsyncOS.

Les clés de fonction ne sont pas activées tant que vous n'activez pas les fonctions respectives.

Création d'adresses IP élastiques

Pour créer une adresse IP élastique, procédez comme suit :

Étape 1 Dans le volet de navigation EC2, cliquez sur **IP Elastic** (IP élastique).

Étape 2 Cliquez sur **Allocate new address** (Allouer une nouvelle adresse).

Étape 3 Cliquez sur **Allocate** (Allouer). Une nouvelle adresse IP publique sera allouée. Vous pouvez soit cliquer sur l'adresse IP, soit cliquer sur **Close** (Fermer).

Étape 4 Sélectionnez l'adresse IP que vous avez créée.

Étape 5 Cliquez sur **Actions** et sélectionnez **Associate Address** (Associer une adresse).

Étape 6 Sélectionnez le **Resource Type** (Type de ressource).

Étape 7 Choisissez l'instance à partir de la liste déroulante.

Étape 8 Choisissez l'adresse IP privée à associer à l'adresse IP élastique.

Étape 9 Cliquez sur **Associate** (Associer).

Étape 10 Cliquez sur **Close** (Fermer).

Configurer l'appliance afin qu'elle envoie des alertes à l'approche de l'expiration de la licence

Consultez l'aide en ligne ou le guide d'utilisation de votre version d'AsyncOS, disponibles à l'emplacement approprié dans Additional Information.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.