Déploiement de Cisco Secure Web Appliance sur la Place de marché Microsoft Azure

Première publication : 2022-07-11

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

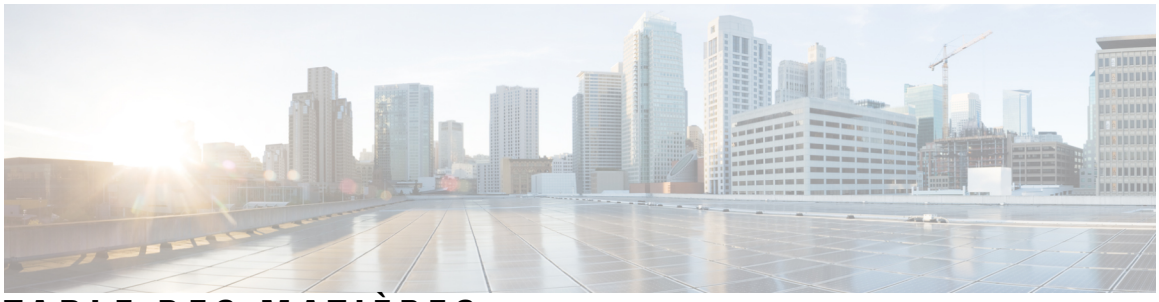
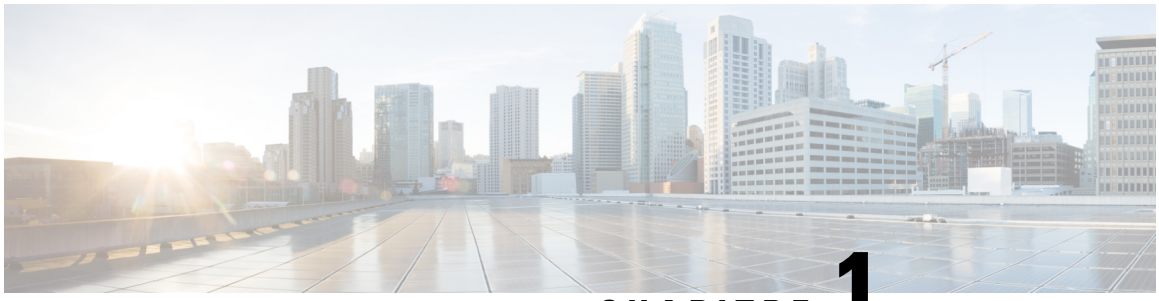


TABLE DES MATIÈRES



CHAPITRE 1

Introduction

À propos de la Place de marché Azure

Vous pouvez utiliser une image d'Azure pour créer une instance de machine virtuelle sur Azure. Les images Azure pour Secure Web Appliance sont disponibles sur la Place de marché Azure.

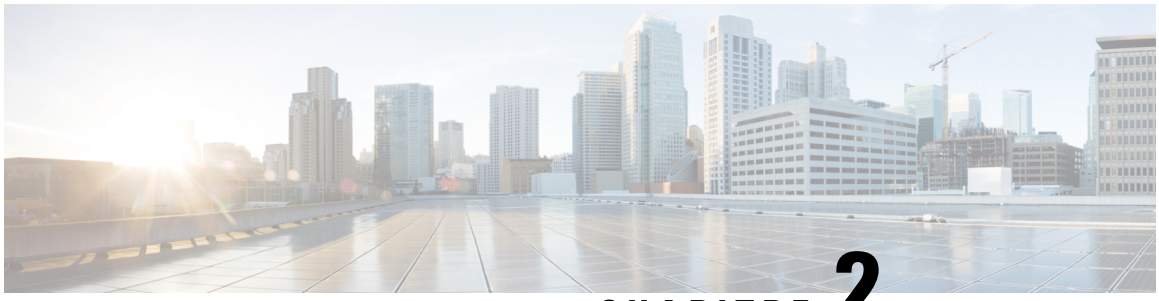
La Place de marché Azure est la première destination pour tous vos besoins en logiciels. Elle est certifiée et optimisée pour fonctionner sur Azure afin de fournir des solutions de bout en bout.

Licences de Secure Web Appliance

Vous pouvez utiliser votre licence existante de Secure Web Appliance pour les déploiements sur Microsoft Azure. Après avoir déployé et lancé l'instance, vous pouvez installer la licence. Vous ne devrez payer que les frais d'infrastructure d'Azure.

Si vous êtes un nouveau client, communiquez avec votre partenaire Cisco pour obtenir une licence.

Si vous êtes déjà un client, consultez la section « Obtain a Virtual License (VLN) » (Obtenir une licence virtuelle [VLN]) dans les notes techniques « Best Practices for Virtual ESA, Virtual WSA, or Virtual SMA Licenses » (Bonnes pratiques pour les licences Virtual ESA, Virtual WSA ou Virtual SMA).



CHAPITRE 2

Déploiement de Secure Web Appliance sur la Place de marché Azure

Vous pouvez déployer Secure Web Appliance sur la Place de marché Azure en utilisant l'interface utilisateur d'Azure et la CLI d'Azure.

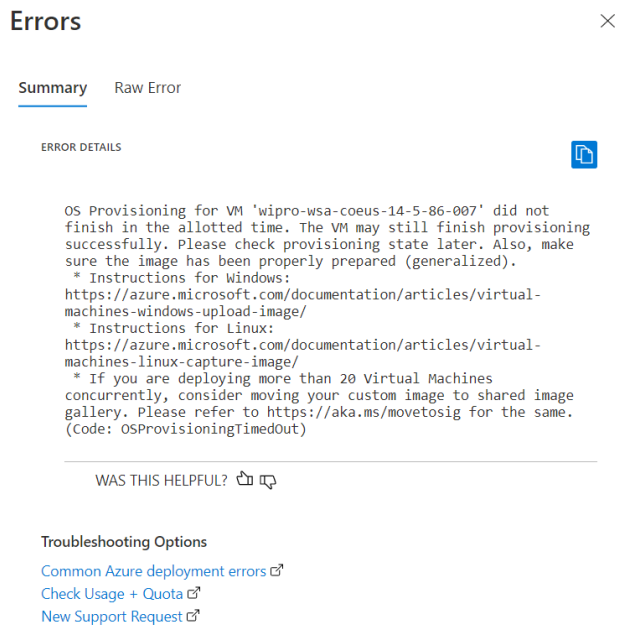
Limites de configuration

- Les configurations suivantes ne sont pas prises en charge pour le déploiement de Secure Web Appliance sur la Place de marché Azure :
  - Moniteur de trafic de couche 4
  - TAP pour traffic Web
- Vous pouvez créer plusieurs interfaces dans l'appliance virtuelle de sécurité Web en utilisant uniquement la CLI de Microsoft Azure.
- À partir de l'interface utilisateur d'Azure, l'instance de Secure Web Appliance peut être configurée avec une seule interface.

Autres renseignements

- L'instance Azure de Secure Web Appliance ne prend pas en charge WAAagent qui est nécessaire pour signaler l'état d'intégrité de l'instance à l'infrastructure Azure. Bien qu'Azure signale un échec de déploiement (délai d'expiration) pour Secure Web Appliance, l'instance sera provisionnée avec succès. Sélectionnez **Boot diagnostics** (Démarrer les diagnostics) pour vérifier l'état actuel de la machine virtuelle.

Illustration 1 : Erreur de mise à disposition



- Les règles de trafic entrant sont l'ensemble de règles qui spécifient s'il faut autoriser ou refuser un trafic spécifique entrant à la machine virtuelle.

  Pour modifier les règles de trafic entrant (accès à Secure Web Appliance) :

  - Sélectionnez l'instance de machine virtuelle souhaitée sous Virtual Machines (Machines virtuelles).
  - Sélectionnez l'option **Networking** (Mise en réseau).

    Vous pouvez maintenant visualiser les règles de trafic entrant répertoriées dans l'interface de gestion.

Remarque Ne supprimez pas les trois règles de sécurité intégrées qui existent déjà.

  Les trois règles de trafic entrant par défaut sont des services spécifiques à Azure comme le réseau virtuel, l'équilibreur de charge et le service qui bloque tout le trafic entrant par défaut, à l'exception de celui qui est autorisé.

- Si les instances sont redémarrées dans Azure, les adresses IP publiques attribuées dynamiquement peuvent être modifiées. Voir la section https://www.linkedin.com/pulse/how-remote-desktop-centos-virtual-machine-running-azure-cretu.
- Bien que l'interface utilisateur d'Azure prenne en charge le déploiement de Secure Web Appliance avec une interface unique, vous pouvez déployer des instances avec plusieurs interfaces en utilisant la CLI d'Azure.

  Pour le déployer des instances Azure avec plus d'une interface, consultez Déploiement de Secure Web Appliance sur l'environnement Azure à l'aide de l'interface de ligne de commande, à la page 9.

Déploiement de Secure Web Appliance sur la Place de marché Azure à l'aide de l'interface utilisateur d'Azure

Remarque Le déploiement de la machine virtuelle est effectué à l'aide de la version provisionnée disponible dans la Place de marché Azure.

Tableau 1 : Déploiement sur Azure à l'aide de l'interface utilisateur

	Faire ceci	Autres renseignements
Étape 1	Préparez votre environnement en effectuant les tâches prérequises et en acquérant les informations dont vous avez besoin avant de configurer une instance dans Azure.	Préparation de votre environnement, à la page 6
Étape 2	Passez à la Place de marché Azure et sélectionnez l'image provisionnée pour la version souhaitée. Cliquez sur **Create** (créer).	Types d'instances prises en charge pour le déploiement, à la page 7.
Étape 3	Sélectionnez le groupe de ressources, le nom et la taille de la machine virtuelle (type d'instance qui diffère selon la RAM et le CPU). Sélectionnez Authentication type (Type d'authentification) comme mot de passe et License type (Type de license) comme Other (Autre) dans l'environnement d'Azure.	Configuration des détails de l'instance, à la page 7
Étape 4	Configurez les options de réseau virtuel, de disque, de sous-réseau et d'adresse IP publique.	Toutes les ressources doivent se trouver dans la même région pour le déploiement.
Étape 5	Créez un groupe de sécurité réseau. Utilisez les règles de trafic entrant par défaut ou ajoutez des règles. Si nécessaire, réglez les **boot diagnostics** (Diagnostics de démarrage) sur **Yes** (Oui). La configuration d'invité est utilisée pour fournir le jour 0.	Configuration des détails de l'instance, à la page 7
Étape 6	Créez des balises comme le nom, le groupe, l'équipe, le modèle et l'objectif selon les exigences.	Configuration des détails de l'instance, à la page 7

	Faire ceci	Autres renseignements
Étape 7	Passez en revue les modifications et déployez l'instance Azure.	L'instance Azure de Secure Web Appliance ne prend pas en charge WAAagent qui est nécessaire pour signaler l'état d'intégrité de l'instance à l'infrastructure Azure. Bien qu'Azure signale un échec de déploiement (délai d'expiration) pour Secure Web Appliance, l'instance est provisionnée avec succès.
Étape 8	Accédez à la page de **Overview** (Vue d'ensemble) de l'instance et vérifiez l'état de l'instance. Il doit être en *Running* (En cours d'exécution). Une adresse IP publique doit être attribuée et peut être utilisée pour se connecter à la console et au navigateur.	
Étape 9	• Accédez à l'instance Azure à partir de la CLI, SSH (à condition que les règles de trafic entrant soient définies sur **Allow** [Autorisation]). • Utilisez la commande **Loadlicense** (Charger une licence) et validez la modification.	• Consultez Préparation de votre environnement, à la page 6 pour connaître les ports requis. • Consultez Configuration d'une instance lancée, à la page 8 pour l'accès SSH et l'accès Web. .
Étape 10	Connectez-vous à l'interface Web de Secure Web Appliance. Vous pouvez exécuter l'assistant de configuration du système, téléverser un fichier de configuration ou configurer les fonctionnalités.	Connexion à l'interface utilisateur de Secure Web Appliance, à la page 9.
Étape 11	Configurez Secure Web Appliance pour recevoir des alertes lors de l'expiration de la licence.	Configurer Secure Web Appliance afin qu'elle envoie des alertes à l'approche de l'expiration de la licence, à la page 9.

Préparation de votre environnement

Pour déployer Secure Web Appliance, vous avez besoin des éléments suivants :

- Une licence valide pour l'appliance virtuelle de sécurité Web.
- Le nom d'utilisateur et le mot de passe par défaut de Secure Web Appliance :
  - Nom d'utilisateur : admin
  - Mot de passe : ironport

Vous pourrez modifier ultérieurement les informations d'authentification par défaut dans l'assistant de configuration du système.

- Ressources requises pour le déploiement d'Azure :
  - Groupe de ressources auquel l'instance appartient
  - Réseau ou sous-réseau virtuel
  - Adresse IP publique (sélectionnée lors de la création de l'instance via l'interface utilisateur)
  - Groupe de sécurité de réseau
  - Règles de trafic entrant et sortant ajoutées au groupe de sécurité du réseau
  - Pour que l'appliance virtuelle ouverte puisse communiquer, utilisez les ports suivants :
    - SSH TCP 22 pour SSH
    - TCP 8443 UI et NGUI
    - TCP 3128
    - TCP 443

Types d'instances prises en charge pour le déploiement

Sélectionnez le type d'instance en fonction du modèle de Secure Web Appliance.

À partir d'AsyncOS 14.5 ou d'une version ultérieure, voici les recommandations pour le déploiement de chaque modèle :

Tableau 2 : Types d'instances prises en charge pour le déploiement

Modèle	Nombre maximal d'interfaces	Azure
S100V, 3 cœurs, 8 Go de RAM, disque de 200 Go	2	Standard_F4s_v2 Standard F4s v2 comporte 4 vCPU et 8 GO de RAM
S300V, 5 cœurs, 12 Go de RAM, disque de 500 Go	4	Standard_F8s_v2 Standard F8s v2 comporte 8 vCPU et 16 Go de RAM
S600V, 12 cœurs, 24 Go de RAM, disque de 750 Go	4	Standard_F16s_v2 Standard F16s v2 comporte 16 vCPU et 32 Go de RAM

Configuration des détails de l'instance

Étape 1 Sélectionnez le groupe de ressources.

Étape 2 Entrez le nom de la machine virtuelle.

Les noms de ressources Azure ne peuvent pas contenir de caractères spéciaux \/""[]:|<>+=;,?*@&, d'espace, et ne peuvent pas commencer par '_' ni se terminer avec '.' ou '-' .

Étape 3 Sélectionnez la région.

Celle-ci sera automatiquement récupérée en fonction du groupe de ressources.

Étape 4 Sélectionnez l'image sur la Place de marché Azure.

Étape 5 Sélectionnez la taille en fonction du modèle à déployer.

Par exemple, le type d'instance F8_S_V2 est recommandé pour le déploiement du modèle S300V.

Étape 6 Sélectionnez le type d'authentification comme mot de passe :

Saisissez n'importe quelle chaîne pour le nom d'utilisateur et le mot de passe.

Remarque Le nom d'utilisateur ne doit pas inclure de mots réservés.

Mais après le déploiement, vous pouvez accéder au **SSH** en utilisant les informations d'authentification par défaut :

- nom d'utilisateur : admin
- mot de passe : ironport

Étape 7 Les ports entrants peuvent être SSH, HTTPS, etc.

Vous pouvez effectuer la même modification dans le groupe de sécurité réseau.

Étape 8 Sélectionnez le type de licence comme **other** (Autre).

Étape 9 Sélectionnez les disques qui peuvent être SSD ou HDD.

Étape 10 Sélectionnez le réseau virtuel et le sous-réseau configuré dans le réseau virtuel.

Étape 11 Activez la configuration de gestion avec le compte de stockage personnalisé.

Étape 12 Ajoutez des balises, puis vérifiez et créez l'instance de la machine virtuelle.

Configuration d'une instance lancée

Étape 1 Dans la barre de recherche, effectuez une recherche filtrée pour un machine virtuelle.

Étape 2 Sélectionnez une machine virtuelle et recherchez son nom.

La machine virtuelle doit être en cours d'exécution avec l'adresse IP publique récupérée.

Étape 3 Configurez le nom DNS personnalisé.

Étape 4 Ajoutez les adresses IP requises aux règles de trafic entrant pour assurer la sécurité des ports requis.

Étape 5 Utilisez un protocole SSH pour vous connecter à une instance en utilisant les informations d'authentification suivantes :

- nom d'utilisateur : admin
- mot de passe : ironport

Étape 6 Ajouter les clés de fonction, au besoin.

Étape 7 Utilisez la commande **Loadlicense** (Charger une licence) pour coller la licence par le biais de la CLI ou chargez-la à partir d'un fichier.

Étape 8 Effectuez la configuration de l'interface et activez le port 8443 pour utiliser l'interface utilisateur à l'aide du nom DNS des machines virtuelles Azure.

Étape 9 Cliquez sur **Commit** (Sauvegarder).

Connexion à l'interface utilisateur de Secure Web Appliance

Utilisez l'interface utilisateur pour configurer le logiciel de l'appliance.

Lorsque vous sélectionnez une instance, l'adresse IP publique s'affiche dans la page **Overview** (Vue d'ensemble). Les informations d'authentification par défaut sont :

- nom d'utilisateur : admin
- mot de passe : ironport

Étape 1 Format pour l'accès Web `https://<hostname>:8443`.

Étape 2 Exécutez l'**assistant de configuration du système**.

Étape 3 Téléversez un fichier de configuration.

Étape 4 Configurez manuellement 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. Consultez Renseignements connexes, à la page 13.

Configurer Secure Web Appliance afin qu'elle envoie des alertes à l'approche de l'expiration de la licence

Pour en savoir plus, consultez la section Managing Alerts (Gestion des alertes) dans le guide d'utilisation d'AsyncOS.

Déploiement de Secure Web Appliance sur l'environnement Azure à l'aide de l'interface de ligne de commande

Vous pouvez déployer Secure Web Appliance dans un environnement Azure à l'aide de l'interface de ligne de commande (CLI).

La marche à suivre pour installer la CLI d'Azure dans différents systèmes d'exploitation est disponible ici : https://docs.microsoft.com/en-us/cli/azure/install-azure-cli.

Dans l'interface utilisateur d'Azure, vous pouvez également trouver Cloud Shell à côté de la barre de recherche. Cloud Shell peut être utilisé pour exécuter les commandes de la CLI d'Azure à partir de l'interface utilisateur d'Azure.

.

Étape 1 Pour vous connecter à votre compte Azure, exécutez les commandes suivantes dans la console Azure :

az login -u <username> -p <password>

az account set --subscription <subscription_id>

L'élément subscription_id peut être obtenu à partir des comptes de stockage.

Étape 2 Pour créer une carte réseau pour l'interface de gestion, exécutez les commandes suivantes :

az network nic create --resource-group <Resource_group_name> --name <M1_interface_name> --vnet-name <Virtual_network>--subnet <Network_name_in_VNET> --network-security-group <NSG_Name>

Étape 3 Pour créer une carte réseau pour l'interface P1, exécutez les commandes suivantes :

az network nic create --resource-group <Resource_group_name> --name <P1_interface_name > --vnet-name <Virtual_network> --subnet <Network_name_in_VNET> --network-security-group <NSG_Name>

Étape 4 Pour créer une adresse IP publique pour l'interface de gestion, exécutez les commandes suivantes :

az network public-ip create --resource-group <Resource_group_name> --name <M1-IP>

Étape 5 Pour créer une adresse IP publique pour l'interface de données, exécutez les commandes suivantes :

az network public-ip create --resource-group <Resource_group_name> --name <P1-IP>

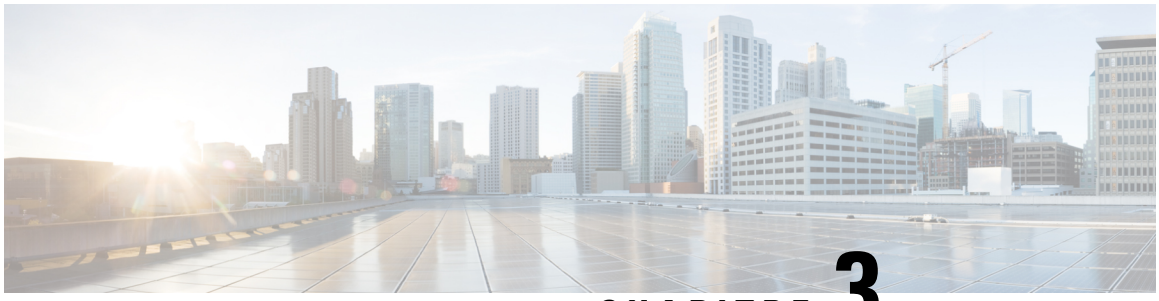
Étape 6 Pour attribuer l'adresse IP publique créée aux interfaces correspondantes, exécutez les commandes suivantes :

az network nic ip-config update --resource-group <Resource_group_name> --nic-name <M1_interface_name> --name ipconfig1 --public-ip <M1-IP>

az network nic ip-config update --resource-group <Resource_group_name> --nic-name <P1_interface_name> --name ipconfig1 --public-ip <P1-IP>

Étape 7 Pour créer une machine virtuelle avec des interfaces de gestion et de données, exécutez les commandes suivantes :

az vm create --resource-group <Resource_group_name> --name <VM_Name> --image <Image_name> --size <instance_type> --admin-username rtestuser --admin-password ironport_123 --nics <M1_interface_name > <P1_interface_name >



CHAPITRE 3

Gestion de l'appliance virtuelle

Commandes de la CLI sur l'appliance virtuelle

Voici les modifications apportées aux commandes de la CLI pour les appliances virtuelles :

Tableau 3 : Commandes de la CLI sur l'appliance virtuelle

Commande	Prise en charge sur Virtual Secure Web Appliance?	Information
loadlicense	Oui	Vous permet d'installer une licence pour votre appliance virtuelle. Vous ne pouvez pas exécuter l'assistant de configuration du système sur l'appliance virtuelle sans installer une licence.
etherconfig	Oui	L'option d'appairage n'est pas incluse sur les appliances virtuelles.
version	Oui	Renvoie toutes les informations de l'appliance virtuelle, à l'exception de l'UDI, du RAID et du BMC.
resetconfig	Oui	Conserve la licence de l'appliance virtuelle et les clés de fonction sur l'appliance.
revert	Oui	Conserve la licence de l'appliance virtuelle et les clés de fonction sur l'appliance.
reload	Oui	Supprime la licence de l'appliance virtuelle et toutes les clés de fonction présentes sur l'appliance. **Remarque** Cette commande est disponible uniquement pour Secure Web Appliance.

Commande	Prise en charge sur Virtual Secure Web Appliance?	Information

diagnostic	Oui	Les options suivantes de sous-menu **diagnostic** > **raid** ne renverront pas d'informations :
		`1. Run disk verify`
		`2. Monitor tasks in progress`
		`3. Display disk verify verdict`
		Remarque Cette commande est disponible uniquement pour Secure Web Appliance.

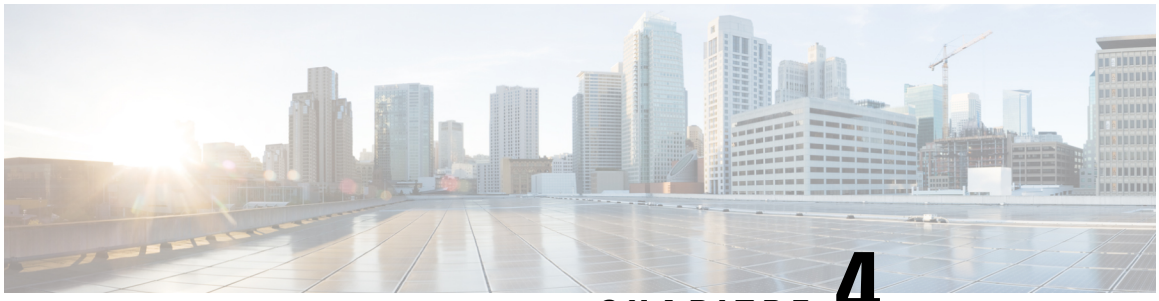
showlicense	Oui	Affiche les détails de la licence. Pour les appliances virtuelles Cisco Secure Web, des informations supplémentaires sont disponibles grâce à la commande **featurekey** (Clé de fonction).

Surveillance Azure

Cette section fournit une prise en charge de la surveillance Microsoft Azure pour Secure Web Appliance

Tableau 4 : Surveillance Azure

Type de moniteur	Prise en charge pour Secure Web Appliance	Commentaires
Aperçus des applications	Non	Vous ne pouvez pas activer les aperçus des applications, car **Update Azure Agent** (Mettre à jour Azure Agent) n'est pas disponible pour Secure Web Appliance.
Alertes	Oui	Les alertes personnalisées et les alertes par défaut sont disponibles.
Journaux	Non	Vous ne pouvez pas activer les aperçus des applications, car **Update Azure Agent** (Mettre à jour Azure Agent) n'est pas disponible pour Secure Web Appliance.
Indicateurs	Oui	—
Paramètres de diagnostic	Non	Vous ne pouvez pas activer **Diagnostic Settings** (Paramètres de diagnostic) pour Secure Web Appliance.



CHAPITRE 4

Renseignements connexes

Renseignements connexes

Pour plus d'informations, y compris des informations sur les options d'assistance, consultez la documentation connexe de votre version d'AsyncOS.

- Guide d'utilisation de Secure Web Appliance
- Notes de mise à jour de Secure Web Appliance
- Guide d'utilisation de Secure Email and Web Manager
- Notes de mise à jour de Secure Email and Web Manager
- Guide d'utilisation de Secure Email Gateway
- Notes de mise à jour de Secure Email Gateway

TAC Cisco

Pour obtenir de l'aide supplémentaire, communiquez avec le centre d'assistance technique (TAC Cisco) à :

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

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.