

Configurer le serveur SMTP pour utiliser AWS SES

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Examiner la configuration AWS SES](#)

[Créer des informations d'identification AWS SES SMTP](#)

[Configurer la configuration SMTP de SNA Manager](#)

[Collecter les certificats AWS](#)

[Configurer l'action de messagerie Response Management](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer votre **Secure Network Analytics Manager (SNA)** à utiliser **Amazon Web Services Simple Email Service (AWS SES)**.

Conditions préalables

Conditions requises

Cisco recommande de connaître ces sujets :

- AWS SES

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- **Stealthwatch Management Console v7.3.2**
- Services AWS SES tels qu'ils existent le 25MAI2022 avec **Easy DKIM**

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Examiner la configuration AWS SES

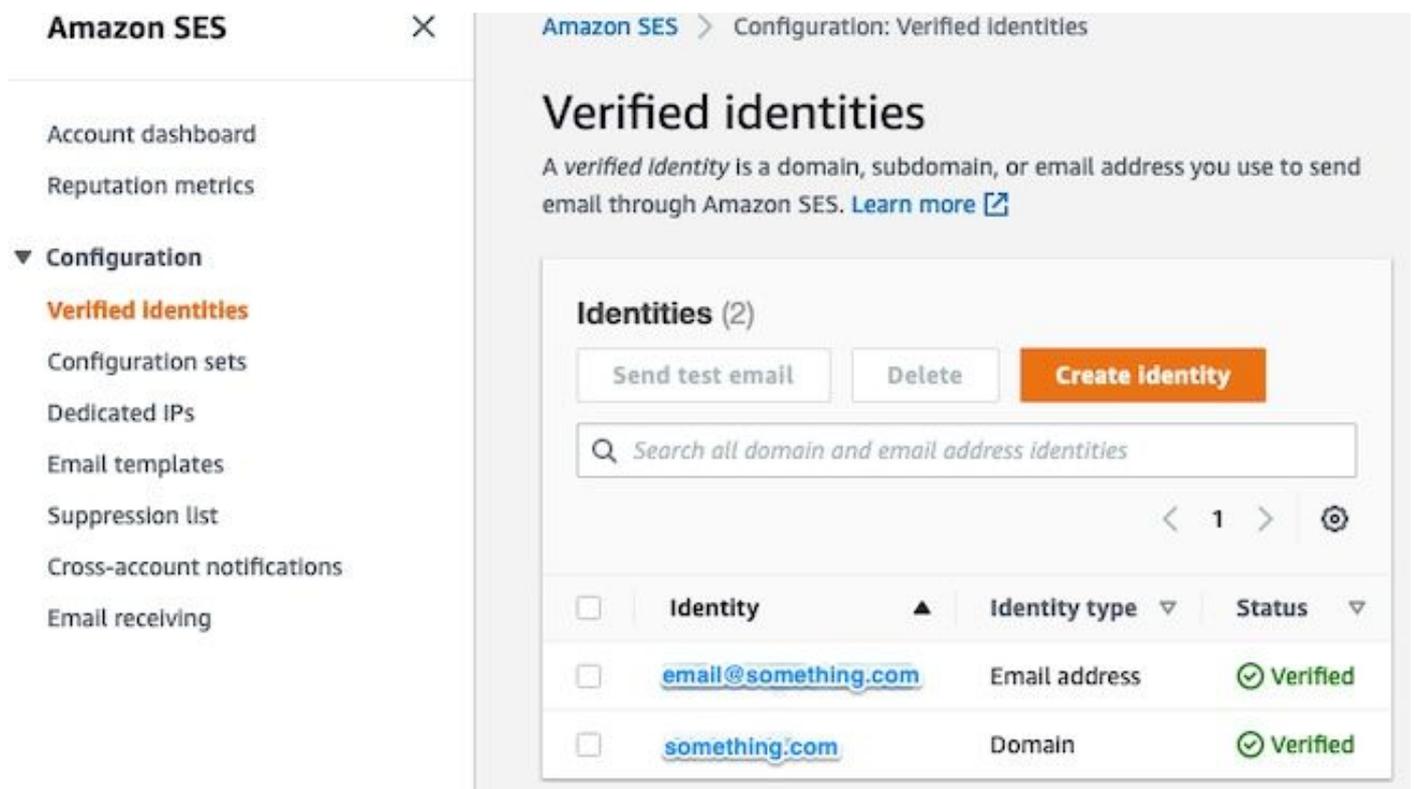
Trois bits d'informations sont requis d'AWS :

1. Emplacement AWS SES
2. Nom d'utilisateur SMTP
3. Mot de passe SMTP

Note: AWS SES situé dans le sandbox est acceptable, mais soyez conscient des limites des environnements de sandbox : <https://docs.aws.amazon.com/ses/latest/dg/request-production-access.html>

Dans la console AWS, accédez à **Amazon SES**, puis sélectionnez **Configuration** et cliquez sur **Verified Identities**.

Vous devez avoir un domaine vérifié. Une adresse e-mail vérifiée n'est pas requise. Reportez-vous à la documentation AWS <https://docs.aws.amazon.com/ses/latest/dg/creating-identities.html#verify-domain-procedure>



The screenshot shows the Amazon SES console interface. On the left is a navigation sidebar with 'Configuration' expanded and 'Verified identities' selected. The main content area is titled 'Verified identities' and includes a description: 'A verified identity is a domain, subdomain, or email address you use to send email through Amazon SES. Learn more'. Below this is a section for 'Identities (2)' with buttons for 'Send test email', 'Delete', and 'Create identity'. A search bar is present with the placeholder 'Search all domain and email address identities'. A table lists the identities:

<input type="checkbox"/>	Identity ▲	Identity type ▼	Status ▼
<input type="checkbox"/>	email@something.com	Email address	✔ Verified
<input type="checkbox"/>	something.com	Domain	✔ Verified

Notez l'emplacement de votre point de terminaison SMTP. Cette valeur est nécessaire ultérieurement.

The screenshot shows the Amazon SES console interface. On the left is a navigation menu with 'Account dashboard' highlighted in orange, and 'Configuration' expanded to show options like 'Verified Identities', 'Configuration sets', 'Dedicated IPs', 'Email templates', 'Suppression list', 'Cross-account notifications', and 'Email receiving'. The main content area is titled 'Simple Mail Transfer Protocol (SMTP) settings'. It includes a brief introduction, a table of settings, and an authentication section.

SMTP endpoint	STARTTLS Port
email-smtp.us-east-1.amazonaws.com	25, 587 or 2587
Transport Layer Security (TLS)	TLS Wrapper Port
Required	465 or 2465

Authentication
You must have an Amazon SES SMTP user name and password to access the SMTP interface. These credentials are different from your AWS access keys and are unique to each region. To manage existing SMTP credentials, [visit the IAM console](#).

[Create SMTP credentials](#)

Créer des informations d'identification AWS SES SMTP

Dans la console AWS, accédez à Amazon SES, puis cliquez sur **Account Dashboard**.

Faites défiler jusqu'à **Simple Mail Transfer Protocol (SMTP) settings** et cliquez sur **Create SMTP Credentials** lorsque vous êtes prêt à terminer cette configuration.

Les informations d'identification plus anciennes et inutilisées (environ 45 jours) ne semblent pas être des informations d'identification incorrectes.

Dans cette nouvelle fenêtre, mettez à jour le nom d'utilisateur avec n'importe quelle valeur et cliquez sur **Create**.

The screenshot shows the 'Create User for SMTP' form. The title is 'Create User for SMTP'. The main text reads: 'This form lets you create an IAM user for SMTP authentication with Amazon SES. Enter the name of a new IAM user or accept the default and click Create to set up your SMTP credentials.' There is a text input field for 'IAM User Name' containing 'ses-stealthwatch-smtp-user' with a note 'Maximum 64 characters'. Below this is a 'Hide More Information' section with explanatory text about IAM user names and SMTP credentials. At the bottom, there is a preview of the IAM policy:

```
"Statement": [{"Effect": "Allow", "Action": "ses:SendRawEmail", "Resource": "*"}]
```

 At the bottom right are 'Cancel' and 'Create' buttons.

Lorsque la page présente les informations d'identification, enregistrez-les. Laissez cet onglet du navigateur ouvert.

Create User for SMTP

☑ **Your 1 User(s) have been created successfully.**

This is the only time these SMTP security credentials will be available for download. Credentials for SMTP users are only available when creating the user. For your protection, you should never share your SMTP credentials with anyone.

▼ [Hide User SMTP Security Credentials](#)

 **ses-stealthwatch-smtp-user**

SMTP Username: AK

SMTP Password: BC

[Close](#)

[Download Credentials](#)

Configurer la configuration SMTP de SNA Manager

Connectez-vous au SNA Manager et ouvrez SMTP Notifications compartiment

1. Open (ouvert) **Central Management > Appliance Manager**.
2. Cliquez sur le bouton **Actions** pour l'appliance.
3. Sélectionner **Edit Appliance Configuration**.
4. Sélectionnez le **General** s'affiche.
5. Faites défiler jusqu'à **SMTP Configuration**
6. Saisissez les valeurs collectées à partir d'**AWS SMTP Server**: Il s'agit de l'emplacement du point de terminaison SMTP collecté dans **SMTP Settings** à partir des versions **AWS SES Account Dashboard** appeler **Port**: Saisissez 25, 587 ou 2587 **From Email**: Cette adresse peut être définie sur n'importe quelle adresse e-mail contenant **AWS Verified Domain** **User Name**: Il s'agit du nom d'utilisateur SMTP présenté à la dernière étape du **Review AWS SES Configuration** compartiment **Password**: Il s'agit du mot de passe SMTP présenté à la dernière étape de la **Review AWS SES Configuration** compartiment **Encryption Type**: Sélectionnez **STARTTLS** (Si vous sélectionnez **SMTPS**, modifiez le port sur 465 ou 2465)
7. Appliquez les paramètres et attendez que le **SNA Manager** retourner à un **UP** état dans **Central Management**

Appliance Configuration - SMC

/ Last Updated: 05/27/2022 10:06 AM by admin

Appliance

Network Services

General

SMTP Configuration ⓘ

SMTP SERVER *

email-smtp.us-east-1.amazonaws.com

PORT

587

FROM EMAIL *

email@something.com

USER NAME

AK

PASSWORD *

ENCRYPTION TYPE

SMTPS STARTTLS UN-ENCRYPTED

Collecter les certificats AWS

Établissez une session SSH vers le **SNA Manager** et connectez-vous en tant qu'utilisateur racine.

Passez en revue ces trois éléments

- Modifier l'emplacement du point de terminaison SMTP (par exemple email-smtp.us-east-1.amazonaws.com)
- Modifiez le port utilisé (par exemple la valeur par défaut 587 pour STARTTLS)
- Les commandes n'ont pas de fonction STDOUT, l'invite est renvoyée une fois l'opération terminée

Pour STARTTLS (port par défaut 587) :

```
openssl s_client -starttls smtp -showcerts -connect email-smtp.us-east-1.amazonaws.com:587 <<<
"Q" 2>/dev/null > mycertfile.crt awk 'split_after == 1 {n++;split_after=0} /-----END
CERTIFICATE-----/ {split_after=1} {print > "cacert" n ".pem"}' < mycertfile.crt for i in `ls -t1
*.pem`; do cp $i $(awk -F "CN=" '/s:/ {gsub(/ /, x); print $NF}' $i).pem ; done ; rm -f cacert*
mycertfile.crt
```

Pour SMTPS (port par défaut 465) :

```
openssl s_client -showcerts -connect email-smtp.us-east-1.amazonaws.com:465 <<< "Q" 2>/dev/null
> mycertfile.crt awk 'split_after == 1 {n++;split_after=0} /-----END CERTIFICATE-----/
{split_after=1} {print > "cacert" n ".pem"}' < mycertfile.crt for i in `ls -tl *.pem`; do cp $i
$(awk -F "CN=" '/s:/ {gsub(/ /,x ); print $NF}' $i).pem ; done ; rm -f cacert* mycertfile.crt
```

Les fichiers de certificat avec l'extension pem sont créés dans le répertoire de travail actuel, ne prenez pas de ce répertoire (sortie de la commande pwd / dernière ligne)

```
sna_manager:~# openssl s_client -starttls smtp -showcerts -connect email-smtp.us-east-
1.amazonaws.com:587 <<< "Q" 2>/dev/null > mycertfile.crt
sna_manager:~# awk 'split_after == 1 {n++;split_after=0} /-----END CERTIFICATE-----/
{split_after=1} {print > "cacert" n ".pem"}' < mycertfile.crt
sna_manager:~# for i in `ls -tl *.pem`; do cp $i $(awk -F "CN=" '/s:/ {gsub(/ /,x ); print $NF}'
$i).pem ; done ; rm -f cacert* mycertfile.crt
sna_manager:~# ll
total 16
-rw-r--r-- 1 root root 1648 May 27 14:54 Amazon.pem
-rw-r--r-- 1 root root 1829 May 27 14:54 AmazonRootCA1.pem
-rw-r--r-- 1 root root 2387 May 27 14:54 email-smtp.us-east-1.amazonaws.com.pem
-rw-r--r-- 1 root root 1837 May 27 14:54 StarfieldServicesRootCertificateAuthority-G2.pem
sna_manager:~# pwd
/root
```

Téléchargez les fichiers créés sur le **SNA Manager** sur votre machine locale avec le programme de transfert de fichiers de votre choix (Filezilla, winscp, etc), et ajoutez ces certificats à la **SNA Manager trust store en Central Management**.

1. Open (ouvert) **Central Management > Appliance Manager**.
2. Cliquez sur le bouton **Actions** pour l'appliance.
3. Sélectionner **Edit Appliance Configuration**.
4. Sélectionnez le **General** s'affiche.
5. Faites défiler jusqu'à **Trust Store**
6. Sélectionner **Add New**
7. Téléchargez chacun des certificats, nous vous recommandons d'utiliser le nom de fichier comme **Friendly Name**

Configurer l'action de messagerie Response Management

Connectez-vous au **SNA Manager**, puis ouvrez la **Response Management** compartiment

1. Sélectionnez le **Configure** dans le ruban principal en haut de l'écran
2. Sélectionner **Response Management**
3. A partir des versions **Response Management** , sélectionnez **Actions** tabulation
4. Sélectionner **Add New Action**
5. Sélectionner **Email** Entrez un nom pour cette action par e-mail Saisissez l'adresse e-mail du destinataire dans le champ « À » (notez que cette adresse doit appartenir au domaine vérifié dans AWS SES) Le sujet peut être n'importe quoi.

Response Management

Rules Actions Syslog Formats

Email Action Cancel Save

Name: AWS SES Test Description:

Enabled Disabled actions are not performed for any associated rules.

To: email@something.com

Subject: AWS SES SMTP Test

Body:

+ Alarm Variables Preview

Test Action

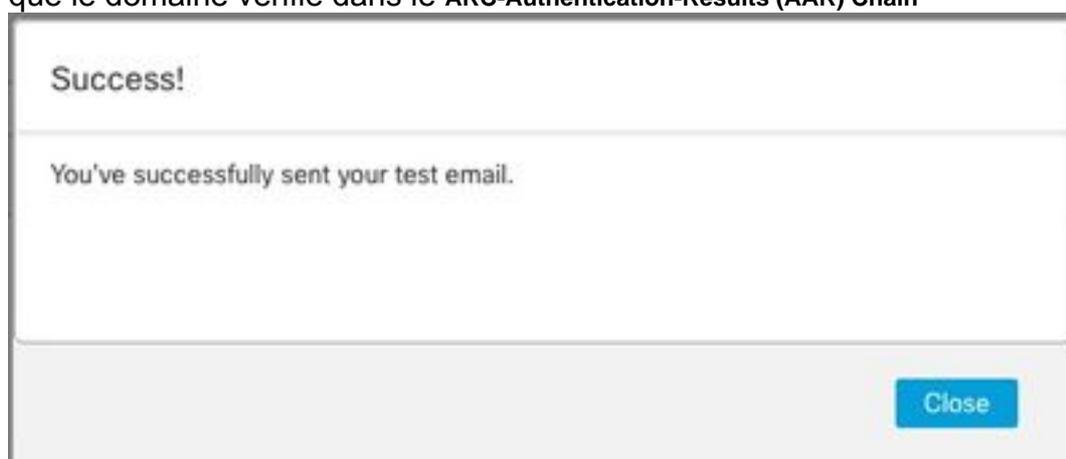
6. Cliquer **Save**

Vérification

Connectez-vous au **SNA Manager**, puis ouvrez la **Response Management** section :

1. Sélectionnez le **Configure** dans le ruban principal en haut de l'écran
2. Sélectionner **Response Management**
3. A partir des versions **Response Management** , sélectionnez **Actions** tabulation
4. Sélectionnez les points de suspension dans la **Actions** pour la ligne de l'action de messagerie que vous avez configurée dans la **Configure Response Management Email Action** , puis sélectionnez **Edit**.
5. Sélectionner **Test Action** et si la configuration est valide, un message de réussite s'affiche et un e-mail est envoyé.

Dans l'en-tête de l'e-mail, amazones est affiché dans le "Received", et des amazones, ainsi que le domaine vérifié dans le **ARC-Authentication-Results (AAR) Chain**



```
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@something.com header.s=
dkim=pass header.i=@amazon.es.com header.
spf=pass (google.com: domain of 010001810
sender) smtp.mailfrom=0100018106685484-fa246764-
Return-Path: <0100018106685484-fa246764-b234-4a
Received: from a8-30.smtp-out.amazon.es.com (a8-
```

- Si le test a échoué, une bannière s'affiche en haut de l'écran. Passez à la section de dépannage

Dépannage

Les `/lancope/var/logs/containers/sw-reponse-mgmt.log` contient les messages d'erreur des actions de test. L'erreur la plus courante, et le correctif est répertorié dans le tableau.

Notez que les messages d'erreur répertoriés dans le tableau ne constituent qu'une partie de la ligne du journal des erreurs

Erreur

SMTPSendFailedException : 554 Message rejeté :
L'adresse e-mail n'est pas vérifiée. Les identités n'ont pas pu être vérifiées dans la région US-EAST-1 :
{adresse_messagerie}

AuthenticationFailedException : 535 Informations d'authentification non valides

Exception SunCertPathBuilder : impossible de trouver un chemin de certification valide vers la cible demandée

Routages SSL : `tls_process_ske_dhe` : clé dh trop petite

Toute autre erreur

Régler

Mettez à jour le message « From Email » dans la configuration SMTP de SNA Manager vers un message appartenant au domaine AWS SES vérifié

Répétez les sections Créer des informations d'identification AWS SES SMTP et Configurer la configuration SMTP de SNA Manager
Confirmer que tous les certificats présentés par AWS se trouvent dans le magasin de confiance SNA Manager - capturer les paquets lorsque l'action de test est exécutée et comparer les certificats présentés par le serveur au contenu du magasin de confiance

Voir addendum

Ouvrir le dossier TAC pour examen

Addenda: Clé DH trop petite.

Il s'agit d'un problème côté AWS, car ils utilisent des clés de 1024 bits lorsque des chiffrements DHE et EDH sont utilisés (risque de bouchon de journal) et que le SNA Manager refuse de poursuivre la session SSL. La sortie de la commande montre les clés de température du serveur de la connexion openssl lorsque des chiffrements DHE/EDH sont utilisés.

```
sna_manager:~# openssl s_client -starttls smtp -connect email-smtp.us-east-2.amazonaws.com:587 -
cipher "EDH" <<< "Q" 2>/dev/null | grep "Server Temp"
Server Temp Key: DH, 1024 bits
sna_manager:~# openssl s_client -starttls smtp -connect email-smtp.us-east-2.amazonaws.com:587 -
cipher "DHE" <<< "Q" 2>/dev/null | grep "Server Temp"
Server Temp Key: DH, 1024 bits
sna_manager:~# openssl s_client -starttls smtp -connect email-smtp.us-east-2.amazonaws.com:587
<<< "Q" 2>/dev/null | grep "Server Temp"
```

Server Temp Key: ECDH, P-256, 256 bits

La seule solution de contournement disponible est de supprimer tous les chiffrements DHE et EDH avec la commande en tant qu'utilisateur racine sur le SMC, AWS sélectionne une suite de chiffrements ECDHE et la connexion réussit.

```
cp /lancope/services/swos-compliance/security/tls-ciphers /lancope/services/swos-compliance/security/tls-ciphers.bak ; > /lancope/services/swos-compliance/security/tls-ciphers ; echo "TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:AES256-GCM-SHA384" > /lancope/services/swos-compliance/security/tls-ciphers ; docker restart sw-response-mgmt
```

Informations connexes

- <https://docs.aws.amazon.com/ses/latest/dg/setting-up.html>
- <https://docs.aws.amazon.com/ses/latest/dg/creating-identities.html#verify-domain-procedure>
- <https://docs.aws.amazon.com/ses/latest/dg/smtp-credentials.html>
- <https://docs.aws.amazon.com/ses/latest/dg/smtp-connect.html>
- [Support et documentation techniques - Cisco Systems](#)