

Configuración del servidor SMTP para utilizar AWS SES

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Revisar configuración de AWS SES](#)

[Crear credenciales SMTP de AWS SES](#)

[Configurar la configuración SMTP del administrador SNA](#)

[Recopilar certificados AWS](#)

[Configurar acción de correo electrónico de administración de respuestas](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar su **Secure Network Analytics Manager (SNA)** para utilizar **Amazon Web Services Simple Email Service (AWS SE)**.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- AWS SES

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- **Stealthwatch Management Console v7.3.2**
- Servicios AWS SES tal y como existen el 25 de MAYO de 2022 con **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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Revisar configuración de AWS SES

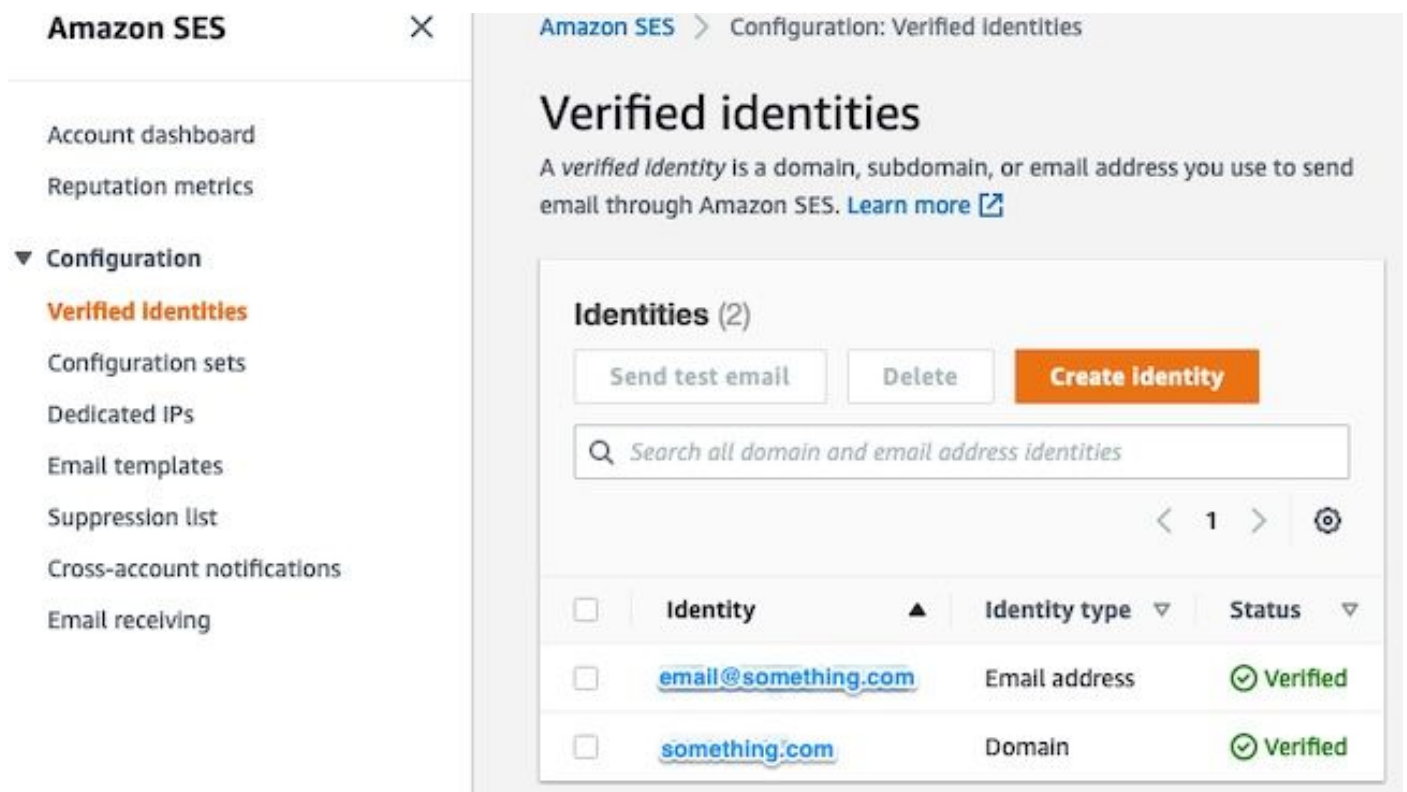
Se requieren tres bits de información de AWS:

1. ubicación de AWS SES
2. Nombre de usuario SMTP
3. Contraseña SMTP

Nota: AWS SES ubicado en el sandbox es aceptable, pero tenga en cuenta las limitaciones de los entornos sandbox: <https://docs.aws.amazon.com/ses/latest/dg/request-production-access.html>

En la consola de AWS, vaya a **Amazon SES**, a continuación, seleccione **Configuration** y haga clic en **Verified Identities**.

Debe tener un dominio verificado. No es necesaria una dirección de correo electrónico verificada. Consulte la documentación de 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 table of identities with two entries: 'email@something.com' (Email address) and 'something.com' (Domain), both with a 'Verified' status. Action buttons like 'Send test email', 'Delete', and 'Create identity' are visible above the table.

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

Observe la ubicación del extremo SMTP. Este valor se necesita más adelante.

Amazon SES X

Simple Mail Transfer Protocol (SMTP) settings

You can use an SMTP-enabled programming language, email server, or application to connect to the Amazon SES SMTP interface. You'll need the following information and a set of SMTP credentials to configure this email sending method in US East (N. Virginia).

SMTP endpoint	STARTTLS Port
<input type="text" value="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](#).

Crear credenciales SMTP de AWS SES

En la consola de AWS, vaya a **Amazon SES**, a continuación, haga clic en **Account Dashboard**.

Desplácese hacia abajo hasta el botón "**Simple Mail Transfer Protocol (SMTP) settings**" y haga clic en **Create SMTP Credentials** cuando esté listo para completar esta configuración.

Las credenciales antiguas no utilizadas (aproximadamente 45 días) no parecen fallar como credenciales no válidas.

En esta nueva ventana, actualice el nombre de usuario a cualquier valor y haga clic en **create**.

Create User for SMTP

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.

IAM User Name:
Maximum 64 characters

▼ **Hide More Information**

Amazon SES uses AWS Identity and Access Management (IAM) to manage SMTP credentials. The IAM user name is case sensitive and may contain only alphanumeric characters and the symbols +=, @- _

SMTP credentials consist of a username and a password. When you click the Create button below, SMTP credentials will be generated for you.

The new user will be granted the following IAM policy:

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


Cuando la página presente las credenciales, guárdelas. Mantenga abierta esta ficha del explorador.

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](#)

Configurar la configuración SMTP del administrador SNA

Inicie sesión en el SNA Managery abra SMTP Notifications sección

1. Abierto **Central Management > Appliance Manager**.
2. Haga clic en el **Actions** para el dispositivo.
3. Seleccionar **Edit Appliance Configuration**.
4. Seleccione el **General** ficha.
5. Desplácese hacia abajo hasta **SMTP Configuration**
6. Introduzca los valores recopilados de **AWS SMTP Server**: Esta es la ubicación del extremo SMTP recopilada de la **SMTP Settings** desde **AWS SES Account Dashboard** página
Port: Introduzca 25, 587 o 2587
From Email: Se puede establecer en cualquier dirección de correo electrónico que contenga el **AWS Verified Domain**
User Name: Este es el nombre de usuario SMTP que se presentó en el último paso del **Review AWS SES Configuration** sección
Password: Ésta es la contraseña SMTP que se presentó en el último paso del **Review AWS SES Configuration** sección
Encryption Type: Seleccione STARTTLS (si selecciona SMTPS, edite el puerto a 465 o 2465)
7. Aplique los parámetros y espere a que **SNA Manager** para volver a una **UP** estado en **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

Recopilar certificados AWS

Establezca una sesión SSH para el **SNA Manager** inicie sesión como usuario raíz.

Revise estos tres elementos

- Cambiar la ubicación del extremo SMTP (por ejemplo, email-smtp.us-east-1.amazonaws.com)
- Cambie el puerto utilizado (por ejemplo, el valor predeterminado de 587 para STARTTLS)
- Los comandos no tienen STDOUT, el mensaje se devuelve al finalizar

Para STARTTLS (puerto predeterminado 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 -tl
*.pem`; do cp $i $(awk -F "CN=" '/s:/ {gsub(/ /,x ); print $NF}' $i).pem ; done ; rm -f cacert*
mycertfile.crt
```

Para SMTPS (puerto predeterminado 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
```

Los archivos de certificado con la extensión pem se crean en el directorio de trabajo actual, no tome de este directorio (salida del comando pwd / última línea)

```
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
```

Descargue los archivos creados en el **SNA Manager** en el equipo local con el programa de transferencia de archivos que elija (Filezilla, winscp, etc.) y agregue estos certificados al **SNA Manager trust store in Central Management**.

1. Abierto **Central Management > Appliance Manager**.
2. Haga clic en el **Actions** para el dispositivo.
3. Seleccionar **Edit Appliance Configuration**.
4. Seleccione el **General** ficha.
5. Desplácese hacia abajo hasta **Trust Store**
6. Seleccionar **Add New**
7. Cargue cada uno de los certificados, se recomienda utilizar el nombre de archivo como **Friendly Name**

Configurar acción de correo electrónico de administración de respuestas

Inicie sesión en el **SNA Manager** y abra el **Response Management** sección

1. Seleccione el **Configure** en la cinta principal de la parte superior de la pantalla
2. Seleccionar **Response Management**
3. Desde **Response Management** página, seleccione **Actions** pestaña
4. Seleccionar **Add New Action**
5. Seleccionar **Email**Proporcione un nombre para esta acción de correo electrónicoIntroduzca la dirección de correo electrónico del destinatario en el campo "Para" (tenga en cuenta que debe pertenecer al dominio verificado en AWS SES)El tema puede ser cualquier cosa.

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

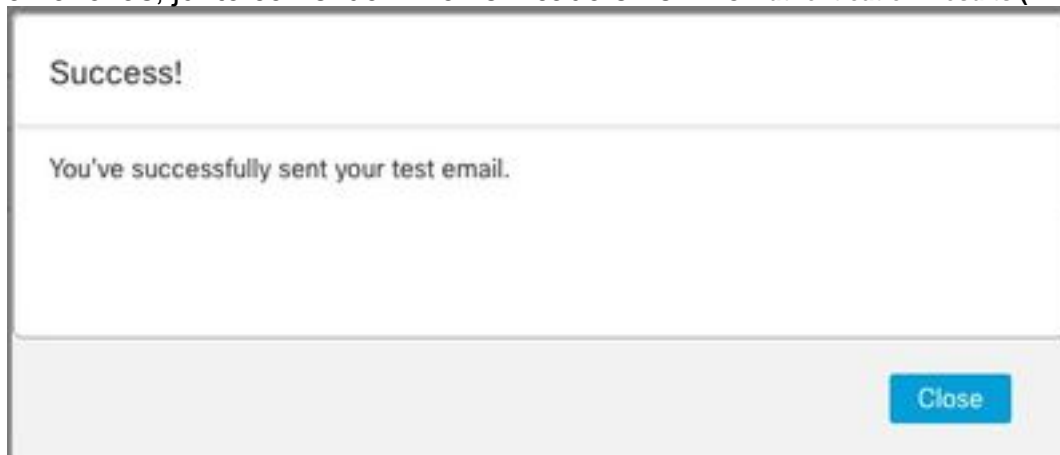
6. Haga clic **Save**

Verificación

Inicie sesión en el **SNA Managery** abra el **Response Management** sección:

1. Seleccione el **Configure** en la cinta principal de la parte superior de la pantalla
2. Seleccionar **Response Management**
3. Desde **Response Management** página, seleccione **Actions** pestaña
4. Seleccione los puntos suspensivos en el **Actions** para la fila de la acción de correo electrónico que ha configurado en el **Configure Response Management Email Action** y seleccione **Edit**.
5. Seleccionar **Test Action** y si la configuración es válida, se presenta un mensaje de confirmación y se envía un correo electrónico.

En el encabezado del correo electrónico, amazonses se muestra en la "Received" y amazonas, junto con el dominio verificado en el **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 la prueba no se realizó correctamente, se muestra un banner en la parte superior de la pantalla: continúe con la sección de solución de problemas

Troubleshoot

`/lancope/var/logs/containers/sw-reponse-mgmt.log` contiene los mensajes de error para las acciones de prueba. El error más común y la corrección se enumeran en la tabla.

Tenga en cuenta que los mensajes de error enumerados en la tabla son sólo una parte de la línea del registro de errores

Error

Excepción SMTPSendFailedException: 554 Mensaje rechazado: La dirección de correo electrónico no se ha verificado. Las identidades no pasaron la comprobación en la región US-EAST-1: {email_address}

Excepción AuthenticationFailedException: 535 Credenciales de autenticación no válidas

Excepción SunCertPathBuilder: no se puede encontrar una ruta de certificación válida para el destino solicitado

rutinas SSL:tls_process_ske_dhe:dh clave demasiado pequeña

Cualquier otro error

Corregir

Actualice el campo "De correo electrónico" de la configuración SMTP del administrador SNA a un correo electrónico que pertenezca al dominio verificado de AWS SES

Repetir secciones Crear credenciales SMTP de AWS SES y Configurar la configuración SMTP del Administrador SNA

Confirme que todos los certificados presentados a AWS estén en el almacén de confianza del Administrador de SNA: realice la captura de paquetes cuando se realice la **Acción de prueba** y compare los certificados presentados en el servidor con el contenido del almacén de confianza

Véase el apéndice

Abrir caso TAC para revisión

Apéndice: La tecla DH es demasiado pequeña.

Este es un problema secundario de AWS, ya que utilizan claves de 1024 bits cuando se utilizan cifrados DHE y EDH (susceptibles de atasco de registro) y el administrador SNA se niega a continuar la sesión SSL. El resultado del comando muestra las claves temporales del servidor de la conexión openssl cuando se utilizan los cifrados DHE/EDH.

```
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 única solución alternativa disponible es eliminar todos los cifrados DHE y EDH con el comando como usuario raíz en el SMC, AWS selecciona un conjunto de cifrados ECDHE y la conexión se realiza correctamente.

```
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
```

Información Relacionada

- <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>
- [Soporte Técnico y Documentación - Cisco Systems](#)