

SMTP-server configureren voor gebruik van AWS SES

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Configuratie AWS SES bekijken](#)

[AWS SES SMTP-referenties maken](#)

[Configuratie SNA Manager SMTP configureren](#)

[AWS-certificaten verzamelen](#)

[E-mailactie voor reactiebeheer configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u uw **Secure Network Analytics Manager (SNA)** voor gebruik **Amazon Web Services Simple Email Service (AWS SES)**.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- AWS SES

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- **Stealthwatch Management Console v7.3.2**
- AWS SES-services zoals deze bestaan op 25 MEI 2022 met **Easy DKIM**

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Configuratie AWS SES bekijken

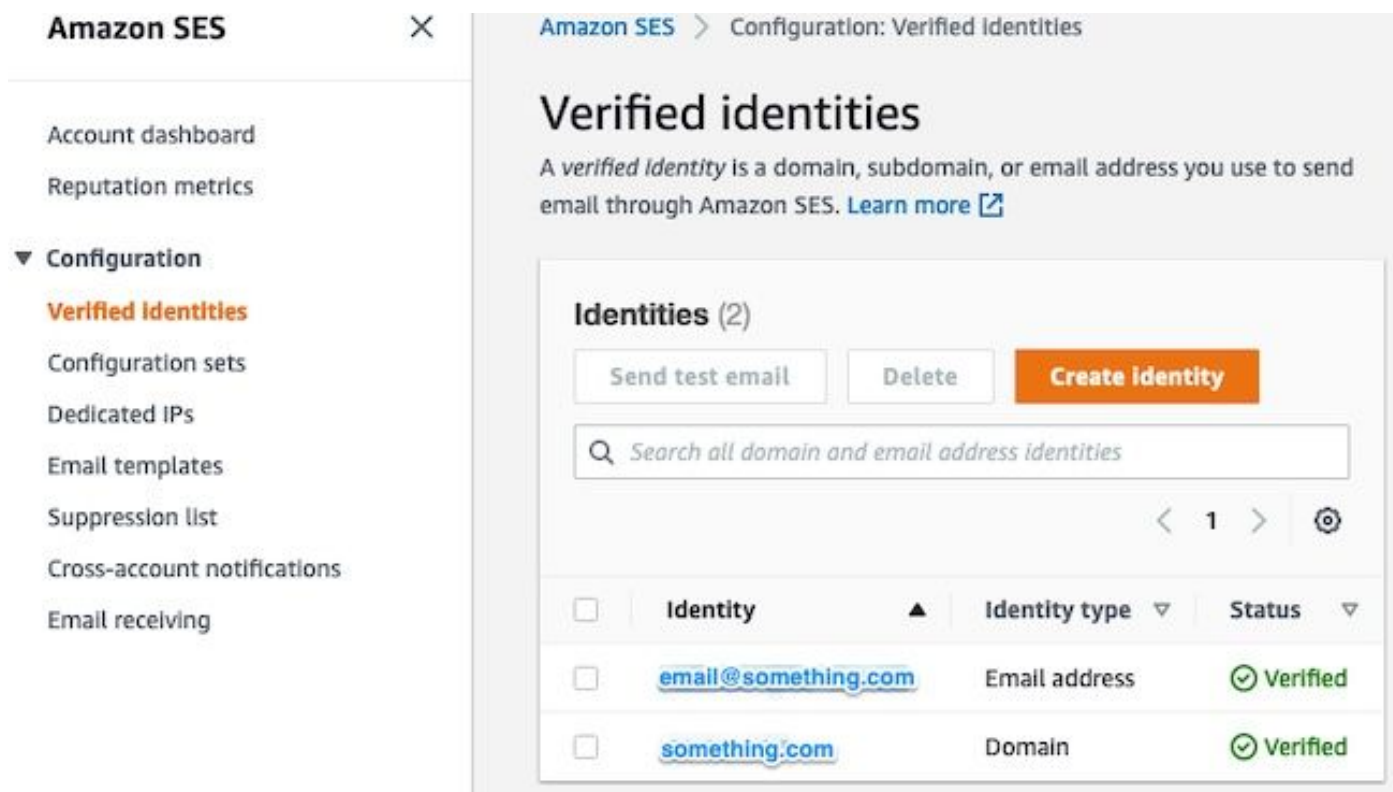
Van AWS worden drie bits informatie vereist:

1. Locatie AWS SES
2. SMTP-gebruikersnaam
3. SMTP-wachtwoord

Opmerking: AWS SES in de zandbak is acceptabel, maar houd rekening met de beperkingen voor zandbakomgevingen: <https://docs.aws.amazon.com/ses/latest/dg/request-production-access.html>

Navigeer in de AWS-console naar **Amazon SES** en selecteer vervolgens **Configuration** en klik op **Verified Identities**.

U moet een geverifieerd domein hebben. Een geverifieerd e-mailadres is niet vereist. Raadpleeg AWS-documentatie <https://docs.aws.amazon.com/ses/latest/dg/creating-identities.html#verify-domain-procedure>



The screenshot shows the AWS SES console interface. On the left is a navigation sidebar with 'Amazon SES' at the top and a 'Configuration' section containing 'Verified identities' (highlighted in orange), 'Configuration sets', 'Dedicated IPs', 'Email templates', 'Suppression list', 'Cross-account notifications', and 'Email receiving'. 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, Verified) and 'something.com' (Domain, Verified). The table has columns for 'Identity', 'Identity type', and 'Status'. Above the table are buttons for 'Send test email', 'Delete', and 'Create identity', along with a search bar and pagination controls.

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

Noteer de locatie van uw SMTP-eindpunt. Deze waarde is later nodig.

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](#).

AWS SES SMTP-referenties maken

Navigeer in de AWS-console naar **Amazon SES** klikt u vervolgens op **Account Dashboard**.

Blader naar beneden naar "**Simple Mail Transfer Protocol (SMTP) settings**" en klik op **Create SMTP Credentials** wanneer u klaar bent om deze configuratie te voltooien.

Oudere, ongebruikte referenties (ongeveer 45 dagen) lijken geen fout te maken als ongeldige referenties.

Werk in dit nieuwe venster de gebruikersnaam bij naar elke waarde en klik op **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": "*"}]
```


Wanneer de pagina de referenties weergeeft, slaat u deze op. Houd deze browser tab open.

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](#)

Configuratie SNA Manager SMTP configureren

Aanmelden bij de SNA Manager, en SMTP Notifications doorsnede

1. Open (Openstaand) **Central Management > Appliance Manager**.
2. Klik op de **Actions** -menu voor het apparaat.
3. Kiezen **Edit Appliance Configuration**.
4. Selecteer de **General** tabblad.
5. Naar beneden bladeren **SMTP Configuration**
6. Voer de uit AWS verzamelde waarden in **SMTP Server**: Dit is de SMTP Endpoint locatie verzameld uit de **SMTP Settings** van de **AWS SES Account Dashboard** pagina
Port: Voer 25, 587 of 2587 in
From Email: Dit kan worden ingesteld op elk e-mailadres dat de **AWS Verified Domain**
User Name: Dit is de SMTP-gebruikersnaam die op de laatste stap in de **Review AWS SES Configuration** doorsnede
Password: Dit is het SMTP-wachtwoord dat op de laatste stap in de **Review AWS SES Configuration** doorsnede
Encryption Type: Selecteer START (Als u SMTPS selecteert, bewerk de poort naar 465 of 2465)
7. Pas de instellingen toe en wacht tot **SNA Manager** om terug te keren naar een UP vermelden in **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

AWS-certificaten verzamelen

Een SSH-sessie instellen voor de **SNA Manager**, en login als wortelgebruiker.

Bekijk deze drie items

- Verander de SMTP-endpointlocatie (bijvoorbeeld email-smtp.us-east-1.amazonaws.com)
- Verander de gebruikte poort (bijvoorbeeld de standaardwaarde van 587 voor STARTTLS)
- De opdrachten hebben geen STDOUT, de prompt wordt na voltooiing teruggegeven

Voor STARTTLS (standaardpoort van 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
```

Voor SMTPS (standaardpoort van 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
```

De certificaatbestanden met de extensie pem worden gemaakt in de huidige werkmap, neem niet van deze map (output van pwd commando / laatste regel)

```
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
```

Download de bestanden die zijn gemaakt op de **SNA Manager** aan uw lokale machine met het programma voor bestandsoverdracht naar keuze (Filezilla, winscp, etc), en voeg deze certificaten toe aan het **SNA Manager trust store** in **Central Management**.

1. Open (Openstaand) **Central Management > Appliance Manager**.
2. Klik op de **Actions** -menu voor het apparaat.
3. Kiezen **Edit Appliance Configuration**.
4. Selecteer de **General** tabblad.
5. Naar beneden bladeren **Trust Store**
6. Kiezen **Add New**
7. Upload elk van de certificaten, aanbevolen om de bestandsnaam als **Friendly Name**

E-mailactie voor reactiebeheer configureren

Aanmelden bij de **SNA Manager**, en opent de **Response Management** doorsnede

1. Selecteer de **Configure** tabblad in het hoofdlint langs de bovenkant van het scherm
2. Kiezen **Response Management**
3. Van de **Response Management** pagina, selecteer **Actions** rekening
4. Kiezen **Add New Action**
5. Kiezen **Email**Een naam voor deze e-mailactie opgevenVoer in het veld "Aan" het e-mailadres van de ontvanger in (let wel: dit moet behoren tot het domein dat in AWS SES is geverifieerd)Het onderwerp kan van alles zijn.

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

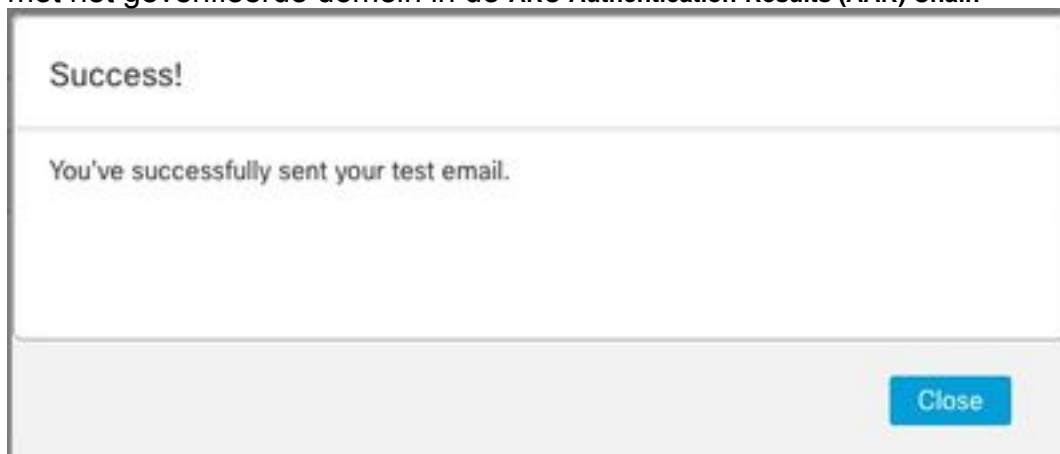
6. Klik **Save**

Verifiëren

Aanmelden bij de **SNA Manager**, en opent de **Response Management** Afdeling:

1. Selecteer de **Configure** tabblad in het hoofdlint langs de bovenkant van het scherm
2. Kiezen **Response Management**
3. Van de **Response Management** pagina, selecteer **Actions** rekening
4. Selecteer de ellips in de **Actions** kolom voor de rij van de e-mailactie die u in de **Configure Response Management Email Action** sectie, en selecteer **Edit**.
5. Kiezen **Test Action** en als de configuratie geldig is, wordt er een succesbericht weergegeven en wordt er een e-mail geleverd.

In de e-mailheader worden amazones getoond in de "Received" veld, en amazones, samen met het geverifieerde domein in de **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-
```

6. Als de test niet succesvol was, wordt er een banner bovenaan het scherm weergegeven - ga verder naar de sectie Problemen oplossen

Problemen oplossen

Het `/lancope/var/logs/containers/sw-reponse-mgmt.log` bestand bevat de foutmeldingen voor de testacties. De meest voorkomende fout, en de fix is vermeld in de tabel. Houd er rekening mee dat de foutmeldingen in de tabel slechts een deel van de foutlogregel vormen

Fout

SMTPSendfailException: Bericht verworpen: E-mailadres niet geverifieerd. De identiteiten zijn niet gecontroleerd in de regio US-EAST-1: {email_adres}

Verificatie misluktExceptie: 535
Verificatiegeloofsgegevens ongeldig

SunCertPathBuilderExceptie: kan geen geldig certificaat vinden voor het gevraagde doel

SSL-routines:tls_process_ske_dhe:dh-toets te klein

Elke andere fout

Oplossen

Werk de "Van E-mail" in de SNA Manager SMTP Configuratie aan een e-mail die tot het AWS SES geverifieerde domein behoort bij

Herhaal secties Maak AWS SES SMTP Credentia
vorm SNA Manager SMTP-configuratie

Bevestig dat alle AWS-voorgestelde certificaten z
SNA Manager trust store bevinden - voer
pakketvastlegging uit wanneer **Test Action** wordt
uitgevoerd en vergelijk server side gepresenteerd
certificaten om de inhoud van de store te vertrou

Zie addendum

Open TAC-case voor review

Addendum: DH-toets te klein.

Dit is een AWS bijzaak, omdat ze 1024 bit-toetsen gebruiken wanneer DHE- en EDH-algoritmen worden gebruikt (logjam vatbaar) en de SNA Manager weigert de SSL-sessie voort te zetten. De opdrachtoutput laat de servertemperatuurtoetsen zien vanaf de openssl-verbinding wanneer DHE/EDH-algoritmen worden gebruikt.

```
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
```


De enige beschikbare tijdelijke oplossing is om alle DHE- en EDH-algoritmen met de opdracht te verwijderen als de hoofdgebruiker op de SMC, AWS selecteert een ECDHE-algoritme en de verbinding slaagt.

```
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_CCM_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
```

Gerelateerde informatie

- <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>
- [Technische ondersteuning en documentatie – Cisco Systems](#)