

# 配置SMTP伺服器以使用AWS SES

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[檢視AWS SES配置](#)

[建立AWS SES SMTP憑證](#)

[配置SNA管理器SMTP配置](#)

[收集AWS證書](#)

[配置響應管理電子郵件操作](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本檔案介紹如何設定 Secure Network Analytics Manager (SNA)使用 Amazon Web Services Simple Email Service (AWS SES)。

## 必要條件

### 需求

思科建議瞭解以下主題：

- AWS SES

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Stealthwatch Management Console v7.3.2
- 2022年5月25日存在的AWS SES服務 Easy DKIM

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 設定

### 檢視AWS SES配置

AWS需要提供三位資訊：

1. AWS SES位置
2. SMTP使用者名稱
3. SMTP密碼

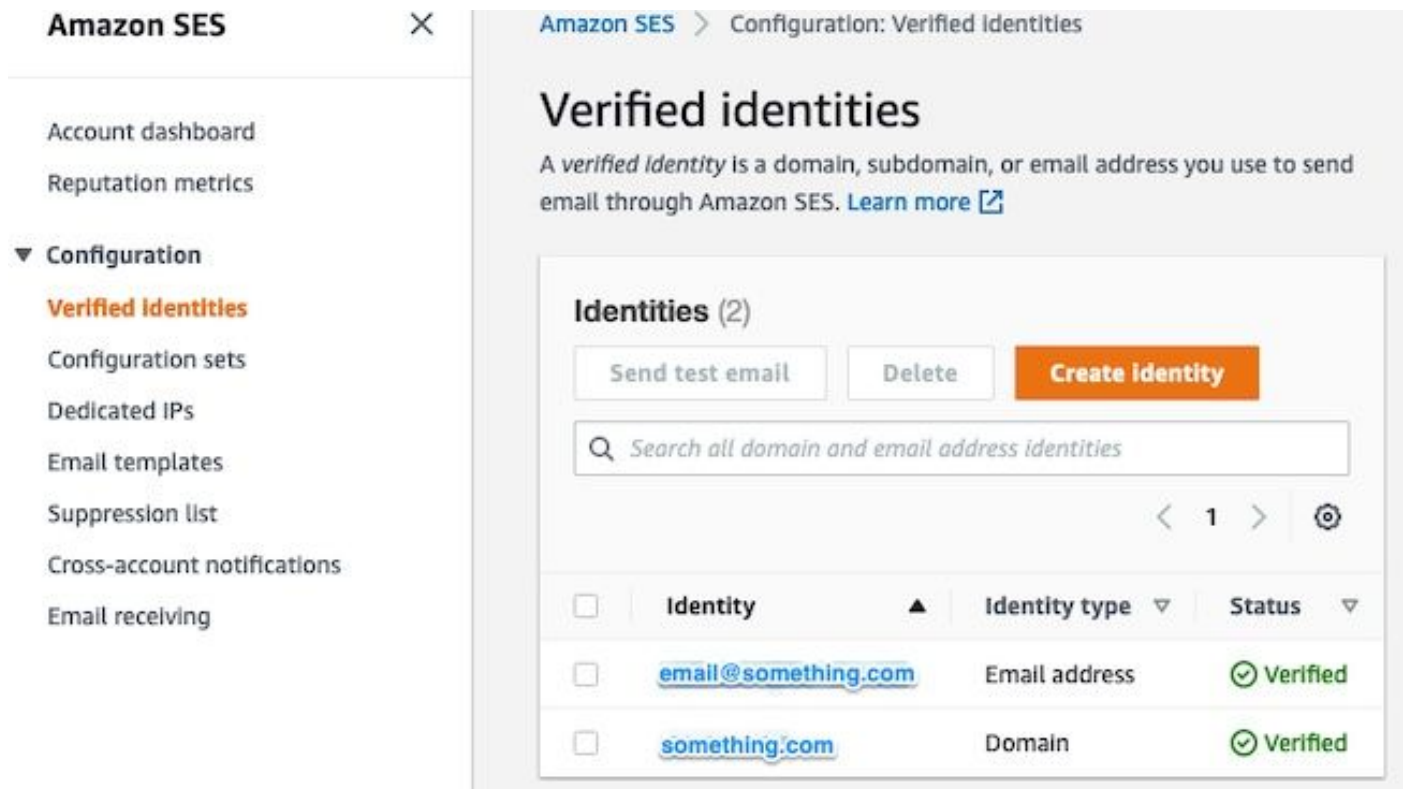
附註：沙盒中的AWS SES是可以接受的，但請注意沙盒環境的限制

：<https://docs.aws.amazon.com/ses/latest/dg/request-production-access.html>

在AWS控制檯中，導航至 Amazon SES，然後選擇 Configuration 然後按一下 Verified Identities。

您必須具有已驗證的域。不需要經過驗證的電子郵件地址。請參閱AWS文檔

<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 options like 'Account dashboard', 'Reputation metrics', and 'Configuration'. The 'Configuration' section is expanded, showing 'Verified Identities' as the active page. 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 text 'Search all domain and email address identities'. At the bottom, there is a table listing the identities.

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

記下SMTP終結點的位置。以後需要此值。

**Amazon SES** ×

**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
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](#)

## 建立AWS SES SMTP憑證

在AWS控制檯中，導航至 Amazon SES，然後按一下 **Account Dashboard**。

向下滾動到「Simple Mail Transfer Protocol (SMTP) settings」並按一下 **Create SMTP Credentials** 當您準備好完成此配置時。

未使用的舊憑據（約45天）似乎不會錯誤為無效憑據。

在此新視窗中，將使用者名稱更新為任意值，然後按一下 **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:** ses-stealthwatch-smtp-user  
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": "*"}]
```

[Cancel](#) [Create](#)

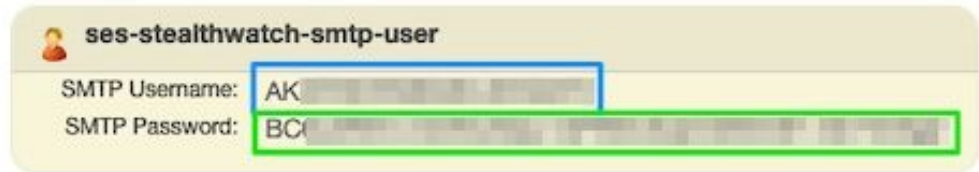
當頁面顯示憑證時，請儲存它們。保持此瀏覽器頁籤開啟。

## 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



The screenshot shows a user creation summary for 'ses-stealthwatch-smtp-user'. It displays the SMTP Username as 'AK' and the SMTP Password as 'BC'. Both fields are highlighted with colored boxes (blue for the username and green for the password).

Close

Download Credentials

## 配置SNA管理器SMTP配置

登入 SNA Manager，然後開啟 SMTP Notifications 部分

1. 未解決 Central Management > Appliance Manager.
2. 按一下 Actions 裝置選單。
3. 選擇 Edit Appliance Configuration.
4. 選擇 General 頁籤。
5. 向下滾動到 SMTP Configuration
6. 輸入從AWS收集的值 SMTP Server:這是從收集的SMTP端點位置 SMTP Settings 從 AWS SES Account Dashboard 頁面Port:輸入25、587或2587From Email:可以將其設定為包含 AWS Verified DomainUser Name:這是在中最後一步上顯示的SMTP使用者名稱 Review AWS SES Configuration 部分Password:這是SMTP密碼，該密碼在中的最後一步出現 Review AWS SES Configuration 部分Encryption Type:選擇 STARTTLS ( 如果選擇SMTPS，請將埠編輯為465或2465 )
7. 應用設定並等待 SNA Manager 要返回到 UP 狀態 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

## 收集AWS證書

建立到 SNA Manager ，並以root使用者身份登入。

檢視這三個專案

- 更改SMTP端點位置(例如email-smtp.us-east-1.amazonaws.com)
- 更改使用的埠 ( 例如 ， STARTTLS的預設埠為587 )
- 命令沒有STDOUT ， 完成後將返回提示

對於STARTTLS ( 預設埠為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
```

對於SMTPS ( 預設埠為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
在當前工作目錄中建立了具有pem副檔名的證書檔案，而不採用此目錄 ( pwd命令輸出/最後一行 )
```

```
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
```

下載在上建立的檔案 **SNA Manager** 使用您選擇的檔案傳輸程式 ( Filezilla、winscp等 ) 將證書新增到本地電腦，並將這些證書新增到 **SNA Manager trust store** 在 **Central Management**.

1. 未解決 **Central Management > Appliance Manager**.
2. 按一下 **Actions** 裝置選單。
3. 選擇 **Edit Appliance Configuration**.
4. 選擇 **General** 頁籤。
5. 向下滾動到 **Trust Store**
6. 選擇 **Add New**
7. 上傳每個憑證，建議使用檔案名稱作為 **Friendly Name**

## 配置響應管理電子郵件操作

登入 **SNA Manager**，然後開啟 **Response Management** 部分

1. 選擇 **Configure** 主功能區中的頁籤
2. 選擇 **Response Management**
3. 從 **Response Management** 頁面，選擇 **Actions** 頁籤
4. 選擇 **Add New Action**
5. 選擇 **Email**為此電子郵件操作提供名稱在「收件人」欄位中輸入收件人電子郵件地址 ( 請注意，此地址必須屬於AWS SES中驗證的域 ) 主題可以是任何東西。

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:

Subject:

Body:

+ Alarm Variables Preview

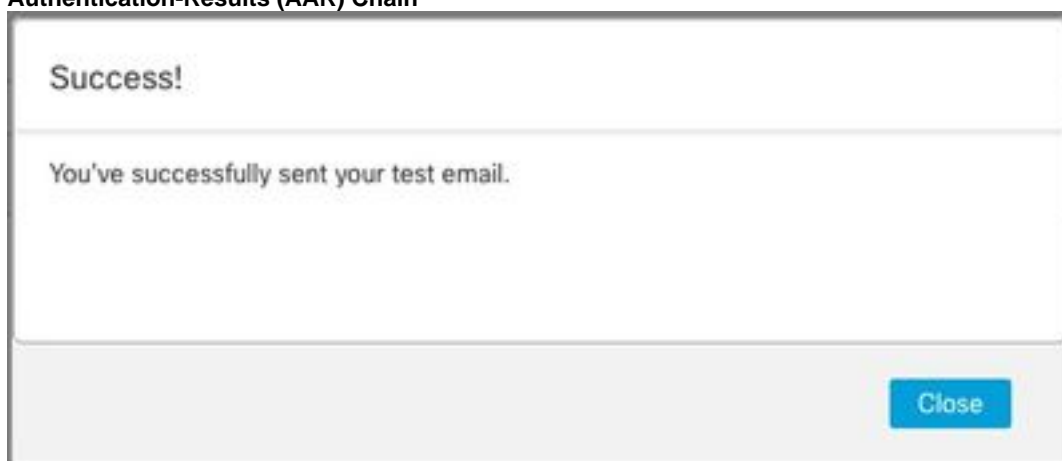
Test Action

6. 按一下 **Save**

## 驗證

登入 **SNA Manager**，然後開啟 **Response Management** 部分：

1. 選擇 **Configure** 主功能區中的頁籤
2. 選擇 **Response Management**
3. 從 **Response Management** 頁面，選擇 **Actions** 頁籤
4. 在 **Actions** 您在中配置的電子郵件操作的行的列 **Configure Response Management Email Action** 部分，然後選擇 **Edit**.
5. 選擇 **Test Action** 如果配置有效，將顯示成功消息並傳送電子郵件。  
在電子郵件標題中，Amazon顯示在「Received」欄位、和amazonses，以及 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.com header.
spf=pass (google.com: domain of 0100018106685484-fa246764-
sender) smtp.mailfrom=0100018106685484-fa246764-
Return-Path: <0100018106685484-fa246764-b234-4a@
Received: from a8-30.smtp-out.amazon.com (a8-
```

6. 如果測試不成功，螢幕頂部將顯示一條橫幅 — 繼續到「疑難解答」部分

## 疑難排解

其 `/lancope/var/logs/containers/sw-reponse-mgmt.log` 檔案包含測試操作的錯誤消息。表中列出了最常見的錯誤以及修補程式。

請注意，表中列出的錯誤消息只是錯誤日誌行的一部分

### 錯誤

SMTPSendFailedException:554郵件被拒絕：未驗證電子郵件地址。身份未通過簽入區域US-EAST-1:{email\_address}

AuthenticationFailedException:535身份驗證憑據無效

SunCertPathBuilderException:無法找到指向所請求目標的有效證書路徑

SSL常式：tls\_process\_ske\_dhe:dh金鑰太小

任何其他錯誤

### 修正

將SNA ManagerSMTP配置中的「從電子郵件」更屬於AWS SES驗證域的電子郵件

重複部分建立AWS SES SMTP憑證和配置SNA Manager SMTP配置

確認所有AWS提供的證書都位於SNA Manager信任存中 — 執行測試操作時執行資料包捕獲，並將伺服器端提供的證書與信任儲存內容進行比較

見增編

開啟需審閱的TAC案例

附約:DH金鑰太小。

這是AWS的一個側問題，因為使用DHE和EDH密碼時，它們使用1024位金鑰（容易發生日誌堵塞），並且SNA Manager拒絕繼續SSL會話。命令輸出會顯示使用DHE/EDH密碼時openssl連線中的伺服器臨時金鑰。

```
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
```

唯一的可用解決方法是以SMC上的根使用者身份使用命令刪除所有DHE和EDH密碼，AWS將選擇ECDHE密碼套件並且連線成功。

```
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_SHA2  
56: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
```

## 相關資訊

- <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>
- [技術支援與文件 - Cisco Systems](#)