

配置SMTP服务器以使用AWS SES

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[查看AWS SES配置](#)

[创建AWS SES SMTP凭证](#)

[配置SNA Manager SMTP配置](#)

[收集AWS证书](#)

[配置响应管理邮件操作](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何配置 Secure Network Analytics Manager (SNA)使用 Amazon Web Services Simple Email Service (AWS SES)。

先决条件

要求

建议掌握下列主题的相关知识：

- AWS SES

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Stealthwatch Management Console v7.3.2
- AWS SES服务于2022年5月25日正式提供， Easy DKIM

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

查看AWS SES配置

AWS需要提供三位信息：

1. AWS SES位置
2. SMTP用户名
3. SMTP密码

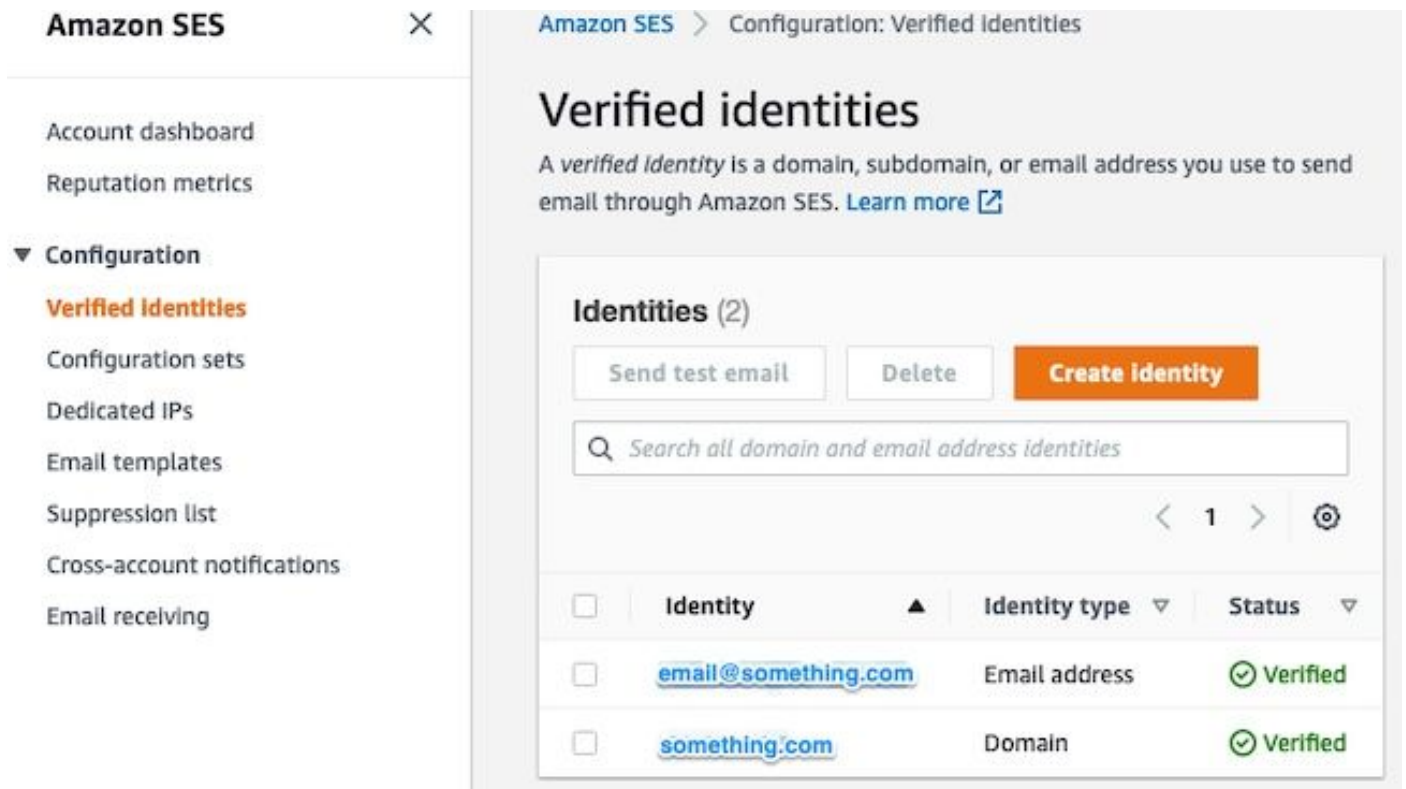
注意：沙盒中的AWS SES是可以接受的，但请注意沙盒环境的限制

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

在AWS控制台中，导航至 Amazon SES,然后选择 Configuration 并点击 Verified Identities.

您必须具有已验证的域。不需要经过验证的邮件地址。请参阅AWS文档

<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 text '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

记下SMTP终结点的位置。稍后需要此值。

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
<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](#).

创建AWS SES SMTP凭证

在AWS控制台中，导航至 **Amazon SES**，然后单击 **Account Dashboard**。

向下滚动到“**Simple Mail Transfer Protocol (SMTP) settings**”并单击 **Create SMTP Credentials** 当您准备好完成此配置时。

未使用的旧凭证（约45天）似乎不会错误为无效凭证。

在此新窗口中，将用户名更新为任意值，然后单击 **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": "*"}]
```

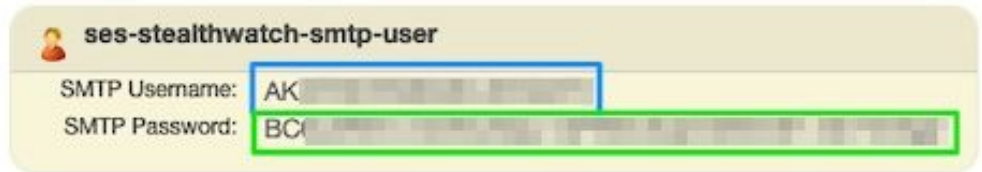
页面显示凭证时，请保存凭证。保持此浏览器选项卡打开。

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 profile card for 'ses-stealthwatch-smtp-user'. It contains two fields: 'SMTP Username' with the value 'AK' and 'SMTP Password' with the value 'BC'. Both fields are highlighted with colored boxes (blue for the username and green for the password).

Close

Download Credentials

配置SNA Manager SMTP配置

登录 SNA Manager ，并打开 SMTP Notifications 部分

1. Open (未解决) Central Management > Appliance Manager.
2. 单击 Actions 菜单中的设置。
3. 选择 Edit Appliance Configuration.
4. 选择 General 选项卡。
5. 向下滚动到 SMTP Configuration
6. 输入从AWS收集的值 SMTP Server:这是从收集的SMTP终端位置 SMTP Settings 从 AWS SES Account Dashboard 页码Port:输入25、587或2587From Email:可以将其设置为包含 AWS Verified DomainUser Name:这是在中最后一步显示的SMTP用户名 Review AWS SES Configuration 部分Password:这是SMTP密码，该密码在中的最后一步出现。 Review AWS SES Configuration 部分Encryption Type:选择 STARTTLS (如果选择SMTPS，请将端口编辑为465或2465)
7. 应用设置并等待 SNA Manager 返回到 UP 状态 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证书

建立与的SSH会话 **SNA Manager** , 并以根用户身份登录。

查看这三个项目

- 更改SMTP端点位置(例如email-smtp.us-east-1.amazonaws.com)
- 更改使用的端口 (例如 , STARTTLS的默认端口为587)
- 命令没有STDOUT , 完成后将返回提示符

对于STARTTLS (默认端口为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
```

对于SMTPS (默认端口为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
在当前工作目录中创建了具有pem扩展名的证书文件，不采用此目录 ( pwd命令的输出/最后一行 )
```

```
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
```

下载在上创建的文件 **SNA Manager** 使用您选择的文件传输程序 (Filezilla、winscp等) 连接到本地计算机，并将这些证书添加到 **SNA Manager trust store** 在 **Central Management**.

1. Open (未解决) **Central Management > Appliance Manager**.
2. 单击 **Actions** 菜单中的设置。
3. 选择 **Edit Appliance Configuration**.
4. 选择 **General** 选项卡。
5. 向下滚动到 **Trust Store**
6. 选择 **Add New**
7. 上传每个证书，建议使用文件名作为 **Friendly Name**

配置响应管理邮件操作

登录 **SNA Manager**，并打开 **Response Management** 部分

1. 选择 **Configure** 选项卡
2. 选择 **Response Management**
3. 从 **Response Management** 页面，选择 **Actions** 选项卡
4. 选择 **Add New Action**
5. 选择 **Email** 为此邮件操作提供名称在“收件人”(To)字段中输入收件人电邮地址 (请注意，此地址必须属于AWS SES中验证的域) 主题可以是任何东西。

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: email@something.com

Subject: AWS SES SMTP Test

Body:

+ Alarm Variables Preview

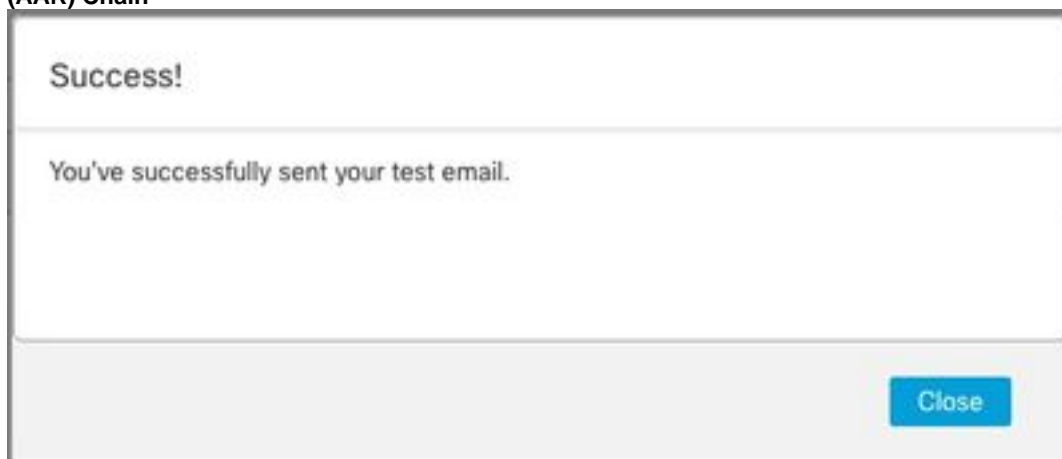
Test Action

6. 点击 **Save**

验证

登录 **SNA Manager**，并打开 **Response Management** 部分：

1. 选择 **Configure** 选项卡
2. 选择 **Response Management**
3. 从 **Response Management** 页面，选择 **Actions** 选项卡
4. 在 **Actions** 中配置的邮件操作所在行的列 **Configure Response Management Email Action** 部分，然后选择 **Edit**.
5. 选择 **Test Action** 如果配置有效，将显示成功消息并发送电子邮件。
邮件信头中的 **amazonses** 显示在“**Received**”字段和 **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 010001810
sender) smtp.mailfrom=0100018106685484-fa246764-
Return-Path: <0100018106685484-fa246764-b234-4a
Received: from a8-30.smtp-out.amazon.com (a8-
```

6. 如果测试不成功，屏幕顶部会显示横幅 — 继续到“故障排除”部分

故障排除

此 `/lancope/var/logs/containers/sw-reponse-mgmt.log` 文件包含测试操作的错误消息。表中列出了最常见的错误和修复方法。

请注意，表中列出的错误消息只是错误日志行的一部分

Error

SMTPSendFailedException:554邮件被拒绝：电子邮件地址未验证。身份未通过区域US-EAST-1的检查
: {email_address}

AuthenticationFailedException:535身份验证凭据无效

SunCertPathBuilderException:找不到到所请求目标的有效证书路径

SSL例程：tls_process_ske_dhe:dh密钥太小

任何其他错误

修复程序

将SNA ManagerSMTP配置中的“从邮件”更新为属AWS SES验证域的邮件

重复部分“创建AWS SES SMTP凭证和配置SNA Manager SMTP配置”

确认所有AWS提供的证书都位于SNA Manager存储中 — 执行测试操作时执行数据包捕获，并将服务器端提供的证书与信任存储内容进行比较

见增编

创建TAC案例供审核

附录:DH密钥太小。

这是AWS方面的一个问题，因为使用DHE和EDH密码（容易发生堵塞）且SNA Manager拒绝继续SSL会话时，它们会使用1024位密钥。命令输出显示使用DHE/EDH密码时来自openssl连接的服务器临时密钥。

```
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
```

唯一可用的解决方法是使用作为SMC上的根用户的命令删除所有DHE和EDH密码，AWS将选择ECDHE密码套件，连接成功。

```
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
```

相关信息

- <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>
- [技术支持和文档 - Cisco Systems](#)