自动导入和导出别名配置

目录

简介

本文档介绍在邮件安全设备内自动执行导入和导出别名配置任务的步骤。

先决条件

要求

建议掌握下列主题的相关知识：

- 思科安全电子邮件网关(SEG/ESA)AsyncOS 16.0.2
- 访问云设备的命令行界面
- Linux CLI
- 外壳脚本

使用的组件

本文档中的信息基于以下软件：

- 云邮件安全设备(CESA)
- 巴什

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。

背景信息

目标是使某些任务自动化，但某些流程通常需要手动干预。但是，在导入和导出当前别名配置时，这些任务可以完全自动化，无需手动输入。

导出和导入别名表

要导入别名表，首先要验证SSH和SCP访问，以确保您可以连接到电子邮件网关。

继续操作之前，别名表必须存在于设备中：

```
(Machine esa1.xyz.iphmx.com) (SERVICE)> clustermode cluster; aliasconfig print

test: test@example.com, test@example2.com, test@example3.com
test2: test@domain.com, test@domain2.com, test@domain3.com
(Cluster Hosted_Cluster) (SERVICE)>
```

使用aliasconfig命令的export子命令备份任何现有别名表时，将生成一个文件（使用您指定的名称），并将其保存在监听程序的/configuration目录中。

使用Bash脚本导出别名表

在这种情况下，bash脚本将连接到CES设备并继续导出别名文件

bash脚本的结构如下所示：

```
#!/bin/bash
```

```
# Configuration of SSH keys and paths
PROXY_KEY="/full/path/folder/.ssh/id_rsa"
SECOND_KEY="/full/path/folder/.ssh/id_rsa"
LOCAL_PORT="2200"
PROXY_USER="dh-user"
PROXY_HOST="f4-ssh.iphmx.com"
TARGET_HOST="esa1.xyz.iphmx.com"
REMOTE_USER="local_server_user"
REMOTE_FILE="/configuration/filename.csv"
LOCAL_DIR="/full/path/folder/Downloads"
LOCAL_FILE_PATH="${LOCAL_DIR}/aliasconfig-file.csv"

# 1. Connect to the proxy and set up the SSH tunnel
echo "Establishing connection to the proxy..."
ssh -i "$PROXY_KEY" -l "$PROXY_USER" -N -f "$PROXY_HOST" -L "$LOCAL_PORT:${TARGET_HOST}:22"
if [ $? -ne 0 ]; then
    echo "Error: Failed to establish connection to the proxy."
    exit 1
fi
echo "Proxy connection established."

# Pause for 5 seconds before proceeding
sleep 5

# 2. Export the aliasconfig file from the remote system
echo "Exporting aliasconfig file from the remote system..."
ssh -i "$SECOND_KEY" "$REMOTE_USER"@127.0.0.1 -p "$LOCAL_PORT" 'clustermode cluster; aliasconfig export
if [ $? -ne 0 ]; then
    echo "Error: Failed to export the aliasconfig file."
    exit 1
fi
echo "Aliasconfig file successfully exported."

# Pause for 5 seconds before proceeding
sleep 5

# 3. Download the file to the local directory
echo "Downloading file to the local directory..."
scp -i "$SECOND_KEY" -P "$LOCAL_PORT" -O "$REMOTE_USER"@127.0.0.1:"$REMOTE_FILE" "$LOCAL_DIR" 2>/dev/nu
if [ $? -ne 0 ]; then
    echo "Error: Failed to download the file to the local directory."
    exit 1
fi
echo "File successfully downloaded to: $LOCAL_FILE_PATH"

# Pause for 5 seconds before finalizing
sleep 5

# Finalizing the script
echo "Process completed successfully."
exit 0
```

说明

1. — 配置SSH密钥和路径

- PROXY_KEY和SECOND_KEY:用于身份验证的SSH私钥文件的完整路径。在这种情况下，两个密钥都设置为相同的路径。
- 示例：/full/path/folder/.ssh/id_rsa
- LOCAL_PORT:指定SSH隧道的本地端口(2200)。
- PROXY_USER:用于连接到代理服务器的用户名。
- PROXY_HOST:代理服务器的主机名。
- TARGET_HOST:目标主机的完全限定域名(FQDN)，更新为esa1.xyz.iphmx.com。
- REMOTE_USER:用于通过SSH隧道连接到远程设备的用户名。
- REMOTE_FILE:远程系统上存储导出文件的路径(/configuration/filename.csv)。
- LOCAL_DIR:用于保存文件的本地目录设置为/full/path/folder/Downloads。
- LOCAL_FILE_PATH:下载文件的完整本地路径，更新为${LOCAL_DIR}/aliasconfig-file.csv。

2. — 连接到代理并设置SSH隧道

```
echo "Establishing connection to the proxy..."
ssh -i "$PROXY_KEY" -l "$PROXY_USER" -N -f "$PROXY_HOST" -L "$LOCAL_PORT:${TARGET_HOST}:22"
```

- 目的:
  — 设置到代理服务器的SSH隧道，以便与目标主机进行安全通信。
- 更新：
  - SSH私钥现在位于/full/path/folder/.ssh/id_rsa。
  — 目标主机名已更新为esa1.xyz.iphmx.com。
- 错误处理：
  — 如果连接失败，将显示错误消息，脚本将退出并显示错误代码(exit 1)。

3. — 暂停5秒后继续

- 目的:
  — 引入延迟，以确保SSH隧道完全建立，然后继续下一步。

4. — 从远程系统导出aliasconfig文件

```
echo "Exporting aliasconfig file from the remote system..."
ssh -i "$SECOND_KEY" "$REMOTE_USER"@127.0.0.1 -p "$LOCAL_PORT" 'clustermode cluster; aliasconfig export
```

- 目的:
  — 通过SSH隧道连接到目标主机，并将别名配置导出到名为aliasconfig-file.csv的文件。
- 更新：
  — 导出文件的文件名已更新为aliasconfig-file.csv。
- 输出重定向：
  - 2>/dev/null抑制来自SSH命令的任何错误消息。

- 错误处理：
  — 如果导出失败，将显示错误消息，脚本将退出。

5. — 将文件下载到本地目录

```
echo "Downloading file to the local directory..."
scp -i "$SECOND_KEY" -P "$LOCAL_PORT" -O "$REMOTE_USER"@127.0.0.1:"$REMOTE_FILE" "$LOCAL_DIR" 2>/dev/nu
```

- 目的:
  — 使用scp将导出文件从远程系统安全地复制到本地目录。
- 更新：
  — 本地文件在/full/path/folder/Downloads目录中另存为aliasconfig-file.csv。
- 错误处理：
  — 如果文件下载失败，将显示错误消息，脚本将退出。

完成脚本

```
echo "Process completed successfully."
exit 0
```

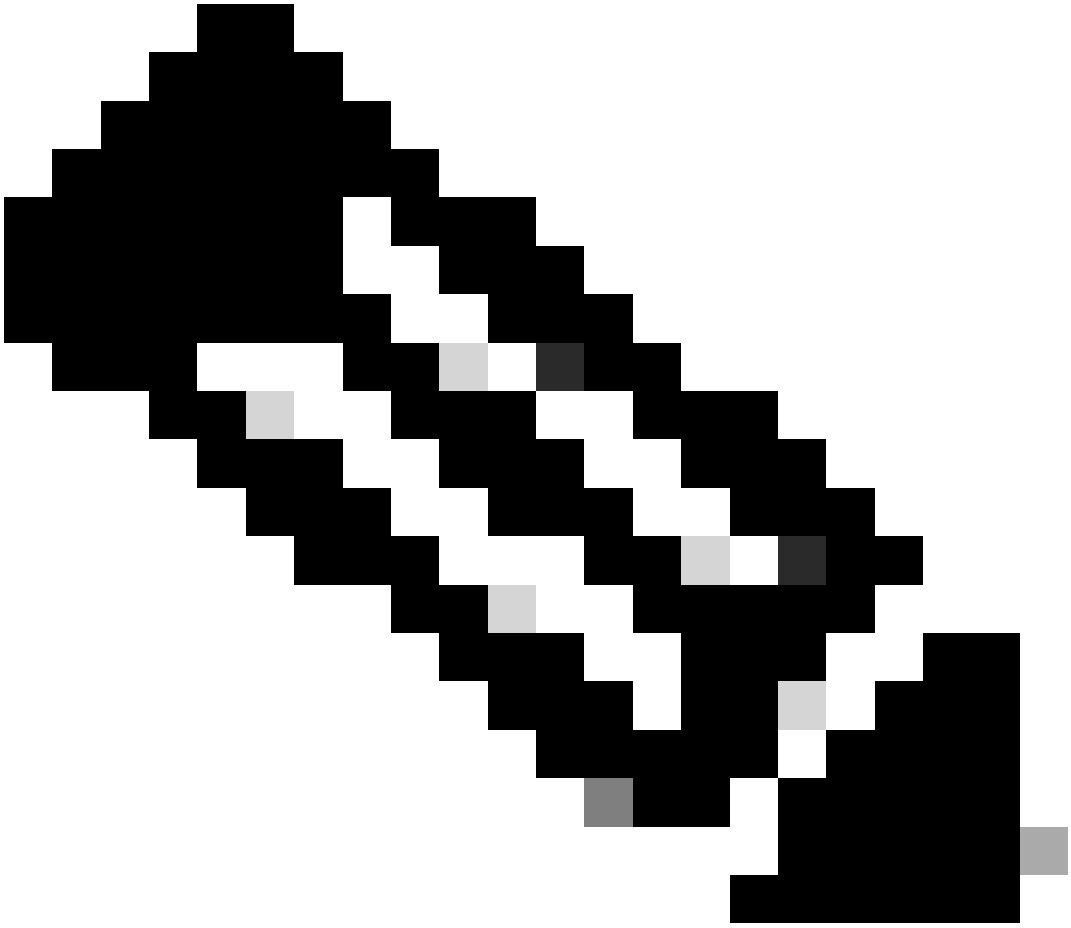
- 目的:
  — 输出成功消息并退出具有成功代码的脚本（退出0），表示所有操作已成功完成。

SSH密钥

您可以在脚本中注意两个变量PROXY_KEY和HOST_KEY。这些密钥可能相同或不同。

PROXY_KEY用于连接到必须跳至CESA服务器的代理云。

HOST_KEY是用于以本地用户身份登录的密钥，无需密码。



注意：要配置对CES代理的SSH访问并为设备上的本地用户设置SSH密钥，请参阅配置指南。

验证导出的文件

执行导出脚本后，您可以验证其内容，并观察其包含的信息与appliance aliasconfig CLI命令中提供的原始信息相同。

```
$ pwd
/full/path/folder/Downloads
$ ls
filename.csv
$ cat filename.csv
# File exported by the CLI at 20250702T125347
test: test@example.com, test@example2.com, test@example3.com
test2: test@domain.com, test@domain2.com, test@domain3.com
```

使用Bash脚本导入别名表

导出当前别名文件后，您可以对其进行修改，添加必要的条目，然后将其导入ESA alia配置。

导入bash脚本的结构如下所示：

```
#!/bin/bash

# Configuration of SSH keys and paths
SSH_KEY="/full/path/folder/.ssh/id_rsa"
LOCAL_PORT="2200"
REMOTE_USER="local_server_user"
LOCAL_FILE="/full/path/folder/Downloads/new-filename.csv"
OUTPUT_DIR="/full/path/folder/Downloads"

# Get the current local date in the desired format
CURRENT_DATE=$(date +"%Y-%m-%d_%H-%M-%S")

# 1. Upload the new aliasconfig file
echo "Uploading new aliasconfig file to the remote system..."
scp -i "$SSH_KEY" -P "$LOCAL_PORT" -O "$LOCAL_FILE" "$REMOTE_USER"@127.0.0.1:/configuration 2>/dev/null
if [ $? -ne 0 ]; then
    echo "Error: Failed to upload the aliasconfig file."
    exit 1
fi
echo "Aliasconfig file successfully uploaded."

# Pause for 5 seconds before proceeding
sleep 5

# 2. Import the new aliasconfig file and commit with a comment
COMMIT_COMMENT="Importing new entries to aliasconfig - $CURRENT_DATE"
echo "Importing the new aliasconfig file and committing changes..."
ssh -i "$SSH_KEY" "$REMOTE_USER"@127.0.0.1 -p "$LOCAL_PORT" "clustermode cluster; aliasconfig import new
if [ $? -ne 0 ]; then
    echo "Error: Failed to import the aliasconfig file or commit changes."
    exit 1
fi
echo "Aliasconfig file successfully imported and committed with comment: '$COMMIT_COMMENT'."

# Pause for 5 seconds before proceeding
sleep 5

# 3. Print the current aliasconfig and save it to a new file
OUTPUT_FILE="${OUTPUT_DIR}/current-aliasconfig-${CURRENT_DATE}.txt"
echo "Printing current aliasconfig and saving it to: $OUTPUT_FILE..."
ssh -i "$SSH_KEY" "$REMOTE_USER"@127.0.0.1 -p "$LOCAL_PORT" 'clustermode cluster; aliasconfig print' >
if [ $? -ne 0 ]; then
    echo "Error: Failed to print the current aliasconfig."
    exit 1
fi
echo "Current aliasconfig successfully saved to: $OUTPUT_FILE"

# Finalizing the script
echo "Process completed successfully."
exit 0
```

说明

1.- SSH路径和密钥配置

- SSH_KEY:SSH私钥文件的路径，用于针对远程服务器进行安全身份验证。
- LOCAL_PORT:为SSH隧道指定的本地端口。
- REMOTE_USER:用于远程服务器上身份验证的用户帐户。
- LOCAL_FILE:要导入的aliasconfig CSV文件的本地路径。
- OUTPUT_DIR:导入过程后保存当前配置副本的本地文件夹。

2. — 获取当前日期和时间

```
CURRENT_DATE=$(date +"%Y-%m-%d_%H-%M-%S")
```

- 目的:
  — 以特定格式存储当前日期和时间，以用于文件名和注释。
- 更新：
  — 通过时间戳轻松跟踪和组织日志和备份。

3. — 将新的aliasconfig文件上传到远程ESA服务器

以下是aliasconfig文件的新内容：

```
# File exported by the CLI at 20250709T112719
test: new-data@example.com, new-date@example2.com, new-date@example3.com
test2: new-date@domain.com, new-data@domain2.com, new-data@domain3.com⏎
```

按照以下说明继续上传文件：

```
echo "Uploading new aliasconfig file to the remote system..."
scp -i "$SSH_KEY" -P "$LOCAL_PORT" -O "$LOCAL_FILE" "$REMOTE_USER"@127.0.0.1:/configuration 2>/dev/null
if [ $? -ne 0 ]; then
    echo "Error: Failed to upload the aliasconfig file."
    exit 1
fi
echo "Aliasconfig file successfully uploaded."
```

- 目的:
  — 使用SCP over SSH将aliasconfig CSV文件从本地计算机传输到远程服务器上的

/configuration目录。
- 更新：
— 如果上传失败，脚本将显示错误并停止以防止导入不完整。

4. — 导入新的aliasconfig文件并使用注释提交

```
COMMIT_COMMENT="Importing new entries to aliasconfig - $CURRENT_DATE"
echo "Importing the new aliasconfig file and committing changes..."
ssh -i "$SSH_KEY" "$REMOTE_USER"@127.0.0.1 -p "$LOCAL_PORT" "clustermode cluster; aliasconfig import new
if [ $? -ne 0 ]; then
    echo "Error: Failed to import the aliasconfig file or commit changes."
    exit 1
fi
echo "Aliasconfig file successfully imported and committed with comment: '$COMMIT_COMMENT'."
```

- 目的:
— 通过SSH连接，将上传的CSV文件导入到别名配置中，并使用带有时间戳的注释提交更改以进行跟踪。
- 更新：
— 如果导入或提交失败，将显示错误消息，脚本将退出以保持配置一致。

5. — 打印当前aliasconfig并将其保存到新的本地文件

```
OUTPUT_FILE="${OUTPUT_DIR}/current-aliasconfig-${CURRENT_DATE}.txt"
echo "Printing current aliasconfig and saving it to: $OUTPUT_FILE..."
ssh -i "$SSH_KEY" "$REMOTE_USER"@127.0.0.1 -p "$LOCAL_PORT" 'clustermode cluster; aliasconfig print' >
if [ $? -ne 0 ]; then
    echo "Error: Failed to print the current aliasconfig."
    exit 1
fi
echo "Current aliasconfig successfully saved to: $OUTPUT_FILE"
```

- •目的:
— 通过SSH连接，打印当前别名配置，并将输出保存到本地时间戳文件，以供备份和审核。
- 更新：
— 如果操作失败，脚本将显示错误并停止以避免给出不完整的结果。

验证更改

执行脚本后，您可以验证别名配置表中的更改，并检查系统日志中的提交。

检验新的aliasconfig表条目

新更改已应用于该表。

```
(Machine esa1.xyz.iphmx.com) (SERVICE)> clustermode cluster; aliasconfig print

test: new-data@example.com, new-data@example2.com, new-data@example3.com
test2: new-data@domain.com, new-data@domain2.com, new-data@domain3.com
```

验证提交更改

此命令允许您跟踪和查看提交到ESA的更改，包括进行更改的用户及其发生日期。

```
(Machine esa1.xyz-66.iphmx.com) (SERVICE)> grep "commit" system_logs
Wed Jul  9 11:29:42 2025 Info: PID 95790: User local_server_user commit changes: Importing new entries
```

脚本灵活性

虽然此脚本当前以Bash编写，但可以轻松地改编或用其他脚本或编程语言（例如Python、PowerShell或Perl）重写，以便更好地与不同管理员和环境的首选项或要求保持一致。这种灵活性可确保能够维护核心逻辑和工作流程，同时利用与您的运营要求最相符的语言或工具。

最终想法

此导入/导出脚本提供了实用有效的解决方案，用于直接在设备上管理别名配置。通过自动上传、导入和备份配置文件，管理员可以安全可靠地引入更改，而无需人工干预。该脚本不仅简化了过程，而且通过带有时间戳的备份和提交注释来确保可跟踪性。

此外，拥有此类脚本还有助于在您的环境中保持一致性和合规性，特别是在需要多次更改或批量更新时。当前配置的定期备份提供了额外的安全层，可根据需要快速恢复或回滚。

总之，此方法使团队能够更有信心、更高效地管理配置更新。对于任何将来的调整，可以轻松调整脚本以处理其他类型的配置文件，或根据需要进一步自动执行其他维护任务。

参考链接

- 访问云邮件安全(CES)解决方案的命令行界面(CLI)
- CLI说明：PuTTY [Windows/PC用户]
- 如何配置SSH公钥身份验证，以便在不使用密码的情况下登录ESA

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。