Azure AD Configuration Script for Cisco Email Security

目錄

簡介

本文檔提供可以從UNIX/Linux環境運行的指令碼，以簡化建立自簽名證書的流程，並在需要配置Cisco電子郵件安全時執行所需的Microsoft Azure步驟。此指令碼可用於郵箱自動補救(MAR)、Microsoft Office 365 LDAP聯結器或Cisco Threat Analyzer for Office 365。此指令碼是獨立的，可與所有版本的AsyncOS for Email Security Appliance(ESA)一起使用。

> **附註**：本文是概念驗證，並提供了示例依據。雖然這些步驟已經過成功測試，但本文主要用於演示和說明目的。自定義指令碼超出思科的範圍和受支援範圍。思科技術支援中心(TAC)不會隨時編寫、更新外部指令碼或對其進行故障排除。在嘗試和構建任何指令碼之前，請確保您在構建最終指令碼時具有指令碼編寫知識。

> **附註**：思科TAC和思科支援人員無權對Microsoft Exchange、Microsoft Azure AD或Office 365的客戶方問題進行故障排除。

必要條件

需求

思科建議您閱讀並瞭解如何為ESA配置Azure AD和Office 365郵箱設定。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

出於此指令碼的目的和執行目的，假設您已安裝了OpenSSL。在終端提示中，執行**哪個openssl**或**openssl版本**以驗證安裝。

為了本文的目的，將以*my_azure.sh*身份呼叫並執行指令碼。您可以隨意命名指令碼。

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。

Azure AD Configuration Script for Cisco Email Security

從外部主機(UNIX/Linux)建立指令碼並複製和貼上以下文本：

```
clear
echo "#############################################################################################
     my_azure.sh by Robert Sherwin (robsherw@cisco.com)  ©2018 Cisco .:|:.:|:.
Using openssl, this script will create a self-signed certificate for you to use in
order to complete the Mailbox Settings configuration for Cisco Email Security.
Please respond to the following prompts:
#############################################################################################
"
if which openssl >/dev/null; then
   echo "openssl check passed: openssl is installed!" & openssl version
else
   echo "You do not appear to have openssl installed." && exit
fi

echo "
Please enter a name for your cert: "
read my_cert

while [ -f $my_cert.key ];
do
   echo "File exists, please enter a name for your cert: " && read my_cert
done

echo "
Thank you.  The files that will be generated for your cert are: "

crt=$my_cert.crt
key=$my_cert.key
pem=$my_cert.pem

echo $crt
echo $key
echo $pem
echo ""

while true; do
   read -p "Are you ready to proceed and generate these files for your configuration? $(tput
smso)(y/n)$(tput sgr0) " yn
   case $yn in
       [Yy]* ) openssl req -x509 -sha256 -nodes -days 1825 -newkey rsa:2048 -keyout $key -out
$crt
openssl rsa -in $key -out $key
cat $key $crt > $pem

echo ""
base64Thumbprint=`openssl x509 -outform der -in $crt | openssl dgst -binary -sha1 | openssl
base64`
base64Value=`openssl x509 -outform der -in $crt | openssl base64 -A`
keyid=`python -c "import uuid; print(uuid.uuid4())"`
echo "
#############################################################################
Next, $(tput smul)copy$(tput rmul) the following to Azure for your manifest:
#############################################################################
"
echo "\"keyCredentials\": [
{
\"customKeyIdentifier\": \"$base64Thumbprint\",
\"keyId\": \"$keyid\",
```

```
\"type\": \"AsymmetricX509Cert\",
\"usage\": \"Verify\",
\"value\": \"$base64Value\"
}
],"
echo "
################################################################################
Then $(tput smul)complete$(tput rmul) the Azure configuration to get the $(tput smso)Client
ID$(tput sgr0) and $(tput smso)Tenant ID$(tput sgr0).
################################################################################
"
echo "This is the $(tput smso)Thumbprint$(tput sgr0) for your ESA configuration:
$base64Thumbprint"
echo "This is the $(tput smso)Certificate Private Key$(tput sgr0) for your ESA configuration:
$pem
"; break;;
       [Nn]* ) exit;;
       * ) echo "Please answer yes or no.";;
   esac
done
while true; do
   read -p "Do you wish to review this certificate in detail? $(tput smso)(y/n)$(tput sgr0) " yn
   case $yn in
       [Yy]* ) openssl x509 -in $crt -text; echo "
Thank you!" && break;;
       [Nn]* ) echo "Thank you!" && exit;;
       * ) echo "Please answer yes or no.";;
   esac
done
```

提示：編寫指令碼後，輸入**chmod u+x <script_name>**使指令碼可執行。

指令碼的完整操作示例應會導致：

```
my_host$ ./my_azure
################################################################################################
     my_azure.sh by Robert Sherwin (robsherw@cisco.com)  ©2018 Cisco .:|:.:|:.
Using openssl, this script will create a self-signed certificate for you to use in
order to complete the Mailbox Settings configuration for Cisco Email Security.
Please respond to the following prompts:
################################################################################################

openssl check passed: openssl is installed!
LibreSSL 2.2.7

Please enter a name for your cert:
technote_example

Thank you.  The files that will be generated for your cert are:
technote_example.crt
technote_example.key
technote_example.pem

Are you ready to proceed and generate these files for your configuration? (y/n) y
Generating a 2048 bit RSA private key
.....................................................+++
.........................................+++
writing new private key to 'technote_example.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:North Carolina
Locality Name (eg, city) []:RTP
Organization Name (eg, company) []:Cisco
Organizational Unit Name (eg, section) []:Example Dept.
Common Name (eg, fully qualified host name) []:example.local
Email Address []:joe.user@example.local
writing RSA key


################################################################################
Next, copy the following to Azure for your manifest:
################################################################################

"keyCredentials": [
{
"customKeyIdentifier": "wWHhkWEfuhDHTXPzzmHoSEnjbNM=",
"keyId": "338836b8-fc8d-4e1b-9a3f-b252f8368d34",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value":
"MIIDtDCCApwCCQDV3bbiHmaN2jANBgkqhkiG9w0BAQsFADCBmzELMAkGA1UEBhMCVVMxFzAVBgNVBAgMDk5vcnRoIENhcm9
saW5hMQwwCgYDVQQHDANSVFAxDjAMBgNVBAoMBUNpc2NvMRYwFAYDVQQLDA1FeGFtcGxlIERlcHQuMRYwFAYDVQQDDA1leGF
tcGxlLmxvY2FsMSUwIwYJKoZIhvcNAQkBFhZqb2UudXNlckBleGFtcGxlLmxvY2FsMB4XDTE4MTAxODAyMDA0OVoXDTIzMTA
xNzAyMDA0OVowgZsxCzAJBgNVBAYTAlVTMRcwFQYDVQQIDA5Ob3J0aCBDYXJvbGluYTEMMAoGA1UEBwwDUlRQMQ4wDAYDVQQ
KDAVDaXNjbzEWMBQGA1UECwwNRXhhbXBsZSBEZXB0LjEWMBQGA1UEAwwNZXhhbXBsZS5sb2NhbDElMCMGCSqGSIb3DQEJARY
Wam9lLnVzZXJAZXhhbXBsZS5sb2NhbDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKlYmW7DN+AxcZQcpc8hZhm
v9yqMHul2cjV3G088mkGtRZU5KUVNKZZSmMlny3lOKg6cTu4Ez4UuigzC/2JXEf3+wOj9YChK92bEYWjYsKeZtbIoqYRfHE+
Sk+bsJb5GpizXgPcYZGje81ecgamhDrg7NZrthPTSKa4ZxmYwpQl6xGDrMipolGoENf+eyNCo5VyAXlxuYH8m6t0GdPw+VKH
J7k+4wI9KTUw4LABoOWs8hUnDi0yz2k9mqNvTG+u75EUUMgcTWc/ISsXjC8kpbOsxteZIiU4xUvqNd1t96iccjad19n61Jds
wGX+CC1Pl+ZZMk8/IQEPtbPqs/4p3cmECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAQqq7ixBbtfhorrWk73uCoYUPRqWZLKH
lgs1UpEnmPjvLZiImY+O6kiR9icDVjFD47AW+0vYg3pHt6pKWl7TUZpilz4hNp0oYc/qjd6aCA8B2KMmbfh2DVhmpYWW8P7w
bNP/im3114F/zJvBVnHjeaY9KsuTUU54Wb8VX2FFX40/YFm/HTHrXcHHyWy5XBU9MFVmEu+Yv6JIxCaEgj5J7jV4qGQM++fn
+EpRPkVHn844Hzgxm40bRW747rjGuyKss+E2tjWJT6OmDJ4ruHCFdvhkZvvzVJyVn0PVN+cwoJ0gLM7p2oa7J3IdNZ3p2CMX
vFdZsRiFFUpBIbK3VYlFRrg=="
}
],

################################################################################
Then complete the Azure configuration to get the Client ID and Tenant ID.
################################################################################

This is the Thumbprint for your ESA configuration: wWHhkWEfuhDHTXPzzmHoSEnjbNM=
This is the Certificate Private Key for your ESA configuration: technote_example.pem
```

指令碼將提示您詳細檢視證書。輸入**y**或**n**以完成指令碼。

```
Do you wish to review this certificate in detail? (y/n) y
Certificate:
   Data:
       Version: 1 (0x0)
       Serial Number: 1541067458222060693 8 (0xd5ddb6e21e668dda)
   Signature Algorithm: sha256WithRSAEncryption
       Issuer: C=US, ST=North Carolina, L=RTP, O=Cisco, OU=Example Dept.,
CN=example.local/emailAddress=joe.user@example.local
       Validity
           Not Before: Oct 18 02:00:49 2018 GMT
           Not After : Oct 17 02:00:49 2023 GMT
```

```
       Subject: C=US, ST=North Carolina, L=RTP, O=Cisco, OU=Example Dept.,
CN=example.local/emailAddress=joe.user@example.local
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
               Public-Key: (2048 bit)
               Modulus:
                   00:a9:58:99:6e:c3:37:e0:31:71:94:1c:a5:cf:21:
                   66:19:af:f7:2a:8c:1e:e9:76:72:35:77:1b:4f:3c:
                   9a:41:ad:45:95:39:29:45:4d:29:96:52:98:c9:67:
                   cb:79:4e:2a:0e:9c:4e:ee:04:cf:85:2e:8a:0c:c2:
                   ff:62:57:11:fd:fe:c0:e8:fd:60:28:4a:f7:66:c4:
                   61:68:d8:b0:a7:99:b5:b2:28:a9:84:5f:1c:4f:92:
                   93:e6:ec:25:be:46:a6:2c:d7:80:f7:18:64:68:de:
                   f3:57:9c:81:a9:a1:0e:b8:3b:35:9a:ed:84:f4:d2:
                   29:ae:19:c6:66:30:a5:09:7a:c4:60:eb:32:2a:68:
                   94:6a:04:35:ff:9e:c8:d0:a8:e5:5c:80:5e:5c:6e:
                   60:7f:26:ea:dd:06:74:fc:3e:54:a1:c9:ee:4f:b8:
                   c0:8f:4a:4d:4c:38:2c:00:68:39:6b:3c:85:49:c3:
                   8b:4c:b3:da:4f:66:a8:db:d3:1b:eb:bb:e4:45:14:
                   32:07:13:59:cf:c8:4a:c5:e3:0b:c9:29:6c:eb:31:
                   b5:e6:48:89:4e:31:52:fa:8d:77:5b:7d:ea:27:1c:
                   8d:a7:75:f6:7e:b5:25:db:30:19:7f:82:0b:53:e5:
                   f9:96:4c:93:cf:c8:40:43:ed:6c:fa:ac:ff:8a:77:
                   72:61
               Exponent: 65537 (0x10001)
   Signature Algorithm: sha256WithRSAEncryption
        42:aa:bb:8b:10:5b:b5:f8:68:ae:b5:a4:ef:7b:82:a1:85:0f:
        46:a5:99:2c:a1:e5:82:cd:54:a4:49:e6:3e:3b:cb:66:22:26:
        63:e3:ba:92:24:7d:89:c0:d5:8c:50:f8:ec:05:be:d2:f6:20:
        de:91:ed:ea:92:96:97:b4:d4:66:98:a5:cf:88:4d:a7:4a:18:
        73:fa:a3:77:a6:82:03:c0:76:28:c9:9b:7e:1d:83:56:19:a9:
        61:65:bc:3f:bc:1b:34:ff:e2:9b:7d:75:e0:5f:f3:26:f0:55:
        9c:78:de:69:8f:4a:b2:e4:d4:53:9e:16:6f:c5:57:d8:51:57:
        e3:4f:d8:16:6f:c7:4c:7a:d7:70:71:f2:5b:2e:57:05:4f:4c:
        15:59:84:bb:e6:2f:e8:92:31:09:a1:20:8f:92:7b:8d:5e:2a:
        19:03:3e:f9:f9:fe:12:94:4f:91:51:e7:f3:8e:07:ce:0c:66:
        e3:46:d1:5b:be:3b:ae:31:ae:c8:ab:2c:f8:4d:ad:8d:62:53:
        e8:e9:83:27:8a:ee:1c:21:5d:be:19:19:be:fc:d5:27:25:67:
        d0:f5:4d:f9:cc:28:27:48:0b:33:ba:76:a1:ae:c9:dc:87:4d:
        67:7a:76:08:c5:ef:15:d6:6c:46:21:45:52:90:48:6c:ad:d5:
        62:51:51:ae
-----BEGIN CERTIFICATE-----
MIIDtDCCApwCCQDV3bbiHmaN2jANBgkqhkiG9w0BAQsFADCBmzELMAkGA1UEBhMC
VVMxFzAVBgNVBAgMDk5vcnRoIENhcm9saW5hMQwwCgYDVQQHDANSVFAxDjAMBgNV
BAoMBUNpc2NvMRYwFAYDVQQLDA1FeGFtcGxlIERlcHQuMRYwFAYDVQQDDA1leGFt
cGxlLmxvY2FsMSUwIwYJKoZIhvcNAQkBFhZqb2UudXNlckBleGFtcGxlLmxvY2Fs
MB4XDTE4MTAxODAyMDA0OVoXDTIzMTAxNzAyMDA0OVowgZsxCzAJBgNVBAYTAlVT
MRcwFQYDVQQIDA5Ob3J0aCBDYXJvbGluYTEMMAoGA1UEBwwDUlRQMQ4wDAYDVQQK
DAVDaXNjbzEWMBQGA1UECwwNRXhhbXBsZSBEZXB0LjEWMBQGA1UEAwwNZXhhbXBs
ZS5sb2NhbDElMCMGCSqGSIb3DQEJARYWam9lLnVzZXJAZXhhbXBsZS5sb2NhbDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKlYmW7DN+AxcZQcpc8hZhmv
9yqMHul2cjV3G088mkGtRZU5KUVNKZZSmMlny3lOKg6cTu4Ez4UuigzC/2JXEf3+
wOj9YChK92bEYWjYsKeZtbIoqYRfHE+Sk+bsJb5GpizXgPcYZGje81ecgamhDrg7
NZrthPTSKa4ZxmYwpQl6xGDrMipolGoENf+eyNCo5VyAXlxuYH8m6t0GdPw+VKHJ
7k+4wI9KTUw4LABoOWs8hUnDi0yz2k9mqNvTG+u75EUUMgcTWc/ISsXjC8kpbOsx
teZIiU4xUvqNd1t96iccjad19n61JdswGX+CC1Pl+ZZMk8/IQEPtbPqs/4p3cmEC
AwEAATANBgkqhkiG9w0BAQsFAAOCAQEAQqq7ixBbtfhorrWk73uCoYUPRqWZLKHl
gs1UpEnmPjvLZiImY+O6kiR9icDVjFD47AW+0vYg3pHt6pKWl7TUZpilz4hNp0oY
c/qjd6aCA8B2KMmbfh2DVhmpYWW8P7wbNP/im3114F/zJvBVnHjeaY9KsuTUU54W
b8VX2FFX40/YFm/HTHrXcHHyWy5XBU9MFVmEu+Yv6JIxCaEgj5J7jV4qGQM++fn+
EpRPkVHn844Hzgxm40bRW747rjGuyKss+E2tjWJT6OmDJ4ruHCFdvhkZvvzVJyVn
0PVN+cwoJ0gLM7p2oa7J3IdNZ3p2CMXvFdZsRiFFUpBIbK3VYlFRrg==
-----END CERTIFICATE-----
```

```
Thank you!
```

此時有三個檔案：.crt、.key和.pem。

按照指示使用*keyCredentials*輸出，並在設定應用註冊時將輸出複製到Azure。在Cisco Email Security上執行組態步驟時，需要*指紋*輸出和*憑證私密金鑰*(.pem)。

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 技術支援與文件 - Cisco Systems