Secuencia de comandos de configuración del Azure AD para la Seguridad del correo electrónico de Cisco

Contenido

Introducción

Este documento proporciona un script que se pueda ejecutar de un entorno UNIX/Linux para simplificar el proceso usado para crear un certificado autofirmado y los pasos requeridos del Microsoft Azure cuando es necesario para configurar la Seguridad del correo electrónico de Cisco. Este script se puede utilizar para la corrección auto del buzón (MARCHA), Microsoft Office el conector de 365 LDAP, o el analizador de la amenaza de Cisco para la oficina 365. Este script es independiente y se puede utilizar con todas las versiones de AsyncOS para el dispositivo de seguridad del correo electrónico (ESA).

> **Note**: Este artículo es un proof-of-concept y con tal que como un ejemplo base. Mientras que estos pasos se han probado con éxito, este artículo se piensa sobre todo para la demostración y los fines de ilustración. Las secuencias de comandos personalizadas están fuera del alcance y de la posibilidad de entretenimiento de Cisco. El Centro de Asistencia Técnica de Cisco (TAC) no escribirá, pondrá al día, o resolverá problemas los scripts externos en cualquier momento. Antes de que usted intente y construya cualquier script, asegúrese de que usted tenga conocimiento del scripting cuando usted construye el script final.

> **Note**: El TAC de Cisco y el soporte de Cisco no se dan derecho a resolver problemas los problemas de lado del cliente con el Microsoft Exchange, el Microsoft Azure AD, o la oficina 365.

Prerrequisitos

Requisitos

Cisco recomienda que usted lee y entiende las configuraciones del buzón del Azure AD y de la oficina 365 de la configuración del Cómo para el ESA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Para el propósito y la ejecución de este script, es bajo suposición que usted hace el OpenSSL instalar. De su prompt terminal, ejecútese **que openssl** o **versión del openssl** para verificar la instalación.

Con el fin de este artículo, el script será llamado y ejecutado como *my_azure.sh*. No dude en para nombrar el script como usted desea.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Secuencia de comandos de configuración del Azure AD para la Seguridad del correo electrónico de Cisco

De un host externo (UNIX/Linux), cree un script y una copia y pegue este texto:

```
borre
produzca eco el
“#############################################################################################
      my_azure.sh de Roberto Sherwin (robsherw@cisco.com) ©2018 Cisco.: |:.: |:.
Usando el openssl, este script creará un certificado autofirmado para que usted utilice adentro
orden para completar la configuración de las configuraciones del buzón para la Seguridad del
correo electrónico de Cisco.
Responda por favor a los prompts siguientes:
#############################################################################################
“
si qué openssl >/dev/null; luego
    control del openssl de la generación de eco “pasajero: el openssl está instalado!” y versión
del openssl

    generación de eco “usted no aparece hacer el openssl instalar.” salida del &&
fi

generación de eco “
Ingrese por favor un nombre para su CERT: “
lea el my_cert

mientras que [-f $my_cert.key];
haga
    archivo de la generación de eco el “existe, satisface ingresa un nombre para su CERT: el” &&
leyó el my_cert
hecho

generación de eco “
Gracias.  Los archivos que serán generados para su CERT son: “

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

```
generación de eco $crt
generación de eco $key
generación de eco $pem
"" de la generación de eco

mientras que es verdad; haga
    ¿leído - p “está usted listo para proceder y para generar estos archivos para su
configuración? $ (tput yn del smso) (y/n)$ (tput sgr0)”
    caso $yn adentro
        [Yy] *) req -x509 -sha256 del openssl - Nodos - días 1825 - newkey rsa:2048 - keyout
$key - hacia fuera $crt
openssl rsa - en $key - hacia fuera $key
gato $key $crt > $pem

"" de la generación de eco
base64Thumbprint=`openssl x509 - der del outform - en $crt | dgst del openssl - -sha1 binario |
openssl base64`
base64Value=`openssl x509 - der del outform - en $crt | base64 del openssl - Un `
pitón del `del keyid= - uuid de la importación c “; print(uuid.uuid4())"`
generación de eco “
################################################################################
Después, $ (smul) del tput copy$ (rmul del tput) el siguiente a Azure para su evidente:
################################################################################
“
“\ “de la generación de eco keyCredentials \”: [
{
\ “más customKeyIdentifier \”: el \"$base64Thumbprint\",
\ “keyId \”: \ “$keyid \”,
\ “tipo \”: el \"AsymmetricX509Cert\",
\ “uso \”: \ “verifique \”,
\ “valor \”: el \"$base64Value\"
}
],”
generación de eco “
################################################################################
Entonces $ (smul) del tput complete$ (rmul del tput) la configuración azul para conseguir el
cliente ID$ (tput sgr0) $ (smso del tput) y al arrendatario ID$ (tput sgr0) $ (smso del tput).
################################################################################
“
produzca eco “esto es el $ (smso) del tput Thumbprint$ (tput sgr0) para su configuración ESA: el
$base64Thumbprint"
produzca eco “esto es el soldado Key$ (tput sgr0) del certificado $ (smso del tput) para su
configuración ESA: $pem
“; rotura; ;
        [Nn] *) salida; ;
        *) la generación de eco “contesta por favor sí o no”; ;
    esac
hecho
mientras que es verdad; haga
    ¿leído - p “usted desea revisar este certificado detalladamente? $ (tput yn del smso) (y/n)$
(tput sgr0)”
    caso $yn adentro
        [Yy] *) openssl x509 - en $crt - texto; generación de eco “
Gracias!” rotura del &&; ;
        [Nn] *) la generación de eco “le agradece!” salida del &&; ;
        *) la generación de eco “contesta por favor sí o no”; ;
    esac
hecho
```

Consejo: Una vez que usted ha escrito el script, ingrese el **<script_name> del chmod u+x** para hacer el script ejecutable.

Un ejemplo completo del script en la acción debe dar lugar a:

```
my_host$ ./my_azure
################################################################################################
      my_azure.sh de Roberto Sherwin (robsherw@cisco.com) ©2018 Cisco.: |:.: |:.
Usando el openssl, este script creará un certificado autofirmado para que usted utilice adentro
orden para completar la configuración de las configuraciones del buzón para la Seguridad del
correo electrónico de Cisco.
Responda por favor a los prompts siguientes:
################################################################################################

control del openssl pasajero: ¡el openssl está instalado!
LibreSSL 2.2.7

Ingrese por favor un nombre para su CERT:
technote_example

Gracias.  Los archivos que serán generados para su CERT son:
technote_example.crt
technote_example.key
technote_example.pem

¿Está usted listo para proceder y para generar estos archivos para su configuración? (y/n) y
Generación de una clave privada de 2048 bits RSA
.......................................................... +++
.......................................... +++
escribiendo la nueva clave privada a “technote_example.key”
-----
Usted está a punto de ser pedido ingresar la información que será incorporada
en su pedido de certificado.
Cuál usted está a punto de ingresar es qué se llama un nombre distintivo o un DN.
Hay muy algunos campos pero usted puede dejar un cierto espacio en blanco
Para algunos campos habrá un valor predeterminado,
Si usted ingresa “. ”, el campo será dejado en blanco.
-----
[]del Nombre del país (2 ponen letras al código): US
[]del nombre del estado o de la provincia (nombre completo): Carolina del Norte
[]del nombre del lugar (eg., ciudad): RTP
[]del nombre de la organización (eg., compañía): Cisco
[]del nombre de la unidad organizacional (eg., sección): Departamento del ejemplo.
[]del Common Name (eg., nombre del host calificado completamente): example.local
[]de la dirección de correo electrónico: joe.user@example.local
escritura de la clave RSA



################################################################################
Después, copie el siguiente a Azure para su evidente:
################################################################################

“keyCredentials”: [
{
“más customKeyIdentifier”: “wWHhkWEfuhDHTXPzzmHoSEnjbNM=”,
“keyId”: el "338836b8-fc8d-4e1b-9a3f-b252f8368d34",
“tipo”: el "AsymmetricX509Cert",
“uso”: “Verifique”,
“valor”:
"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=="
}
],

################################################################################
Entonces complete la configuración azul para conseguir el ID de cliente y al arrendatario ID.
################################################################################

Éste es el Thumbprint para su configuración ESA: wWHhkWEfuhDHTXPzzmHoSEnjbNM=
Ésta es la clave privada del certificado para su configuración ESA: technote_example.pem
```

El script le indicará a que revise el certificado detalladamente. Ingrese **y** o **n** para completar el script.

```
¿Usted desea revisar este certificado detalladamente? (y/n) y
Certificado:
    Datos:
        Versión: 1 (0x0)
        Número de serie: 15410674582220606938 (0xd5ddb6e21e668dda)
    Algoritmo de la firma: sha256WithRSAEncryption
        Emisor: C=US, ST= Carolina del Norte, L=RTP, O=Cisco, departamento de OU=Example,
CN=example.local/emailAddress= joe.user@example.local
        Validez
            No antes: 18 de octubre 02:00:49 2018 GMT
            No después: 17 de octubre 02:00:49 2023 GMT
        Asunto: C=US, ST= Carolina del Norte, L=RTP, O=Cisco, departamento de OU=Example,
CN=example.local/emailAddress= joe.user@example.local
        Información de clave pública sujeta:
            Algoritmo de la clave pública: rsaEncryption
                Clave pública: (2048 mordidos)
                Módulo:
                    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
                Exponente: 65537 (0x10001)
    Algoritmo de la firma: 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
-----COMIENCE EL CERTIFICADO-----
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==
-----TERMINE EL CERTIFICADO-----

¡Gracias!
```

Ahora, usted tiene tres archivos: .crt, .key, y .pem.

Utilice los *keyCredentials* hechos salir según lo dado instrucciones, y copie la salida a Azure cuando usted configura el registro del App. La salida de *Thumbprint* y la *clave privada del certificado* (.pem) son necesarias cuando usted funciona con los pasos para la configuración en la Seguridad del correo electrónico de Cisco.

Información Relacionada

- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems