VMware ESXi へのカスタム証明書(プライベートCA)更新方法

【やりたい事】
VMware ESXi 管理画面にアクセス(https)する際に、証明書エラーが発生するので、
プライベートCAの証明書に変更する事で、証明書エラーを出ないようにする。

【前提条件】
・プライベートCAの構築/運用を行っていること。
 → 自己署名証明書を使う手法もあるが、プライベートCAから発行した証明書を利用
 → プライベートCAは、openssslコマンドで発行している
 → 証明書チェーンは、ROOTCA証明書->中間CA証明書->サーバー証明書(ESXi)
 → サーバー証明書(ESXi)のCNは、192.168.100.1 のIPアドレス用証明書とする
 → 内部DNSサーバーで名前解決する方法もあるが、今回はIPアドレス用証明書を利用

・ROOTCA証明書は、利用するブラウザにインポート済であること

【環境】
・VMware ESXi 6.7.0 Update 3
 → 個人利用の為、ｖCenterはありません。
・FireFox 104.0.2 (64 ビット)
・OpenSSL 1.1.1k

【手順】

(1) サーバー証明書を発行し、プライベートCAの署名を行う。

(1-1) ESXiにSSHログインを行い、/etc/vmware/ssl/rui.key を取得。

[ESXi] # cat /etc/vmware/ssl/rui.key
※ 今回、秘密鍵ファイルは変更(再作成)しないので、そのまま利用

(1-2) CSR作成とCA署名の実施

[PCA] # vi /tmp/esxi.example.jp.key
(1-1)のデータをコピペ＆保存

[PCA] # cd /root
openssl req -new -key /tmp/esxi.example.jp.key -out /tmp/esxi.example.jp.csr
(DN情報を入れる)

CSRが出来上がったら、プライベートCAで署名する。
=> 署名後のファイルを取得しておく。(esxi.example.jp.pem)

※CA署名時のポイント※
X509v3拡張情報として、SAN (SubjectAltName)をCA側(openssl.cnf)で追加する。
SubjectAltName = DNS.1: esxi.example.jp,IP.1: 192.168.100.1

FireFoxでは、「DNS: 192.168.100.1」とDNS属性しても証明書エラーが発生するので、
「IP: 192.168.100.1」IP属性にする必要があった。

(1-3) 中間CA証明書の取得

[PCA] # cat /opt/privateca/ICA/cacert.pem

(2) ESXiにて証明書ファイルを変更する

© 2026 netstaff <netstaff@chovits.net> | 2026-11-22 23:23
URL: https://www.chovits.jp/phpmyfaq/content/0cat=1/17/ja/vmware-esxi-へのカスタム証明書プライベートca更新方法.html

(2-1) 念のため、改修するファイルのバックアップを取得する

ESXi上では、
サーバー証明書ファイル ： rui.crt
サーバー証明書鍵ファイル： rui.key

cd /etc/vmware/ssl
mv rui.crt rui.crt.bak

vi rui.crt
(1-2)で取得したサーバー証明書ファイル(esxi.example.jp.pem)を貼り付け
(1-3)で取得した中間CA証明書を貼り付け
貼り付け順番は、サーバー証明書、中間CA証明書の順

ex) ESXi上にファイルとして保存した場合、

サーバー証明書：/tmp/esxi.example.jp.pem
中間CA証明書 ：/tmp/cacert.pem

[ESXi] # cat /tmp/esxi.example.jp.pem /tmp/cacert.pem > /etc/vmware/ssl/rui.crt

(2-2) プロセス再起動と変更内容をシステム ディスクに保存操作を行う。

/etc/init.d/hostd restart
/etc/init.d/vpxa restart
/sbin/auto-backup.sh

※ 当環境では、OS再起動を行わずにプロセス再起動で対応しているが、
正規手順は、ESXiの再起動を行う事になっているので、あくまで参考程度とすること。

ESXi Shell からのデフォルトの証明書とキーの置き換え
https://docs.vmware.com/jp/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-A261E6D8-03E4-48ED-ADB6-473C2DAAB7AD.html

(3) 掃除

[PCA] # rm /tmp/esxi.example.jp.key
rm /tmp/esxi.example.jp.csr
rm /tmp/esxi.example.jp.pem

※ 証明書データをコピペせずに、ESXi上にファイル転送(保存)した場合は、一時保存した(不要な)ファイルを削除すること

添付ファイル::

一意的なソリューション ID: #1016
製作者: n/a
最終更新: 2022-09-16 10:24

© 2026 netstaff <netstaff@chovits.net> | 2026-11-22 23:23
URL: https://www.chovits.jp/phpmyfaq/content/0cat=1/17/ja/vmware-esxi-へのカスタム証明書プライベートca更新方法.html