Hvrsslgen

Contents

Name

hvrsslgen - Generate a private key and public certificate pair.

Synopsis

hvrsslgen [*-options*] *basename subj*

Description

Command **hvrsslgen** generates a private key and public key pair required for SSL Connection. These key files together are required for establishing a secure encrypted connection between HVR hub and remote HVR locations. Both files (private key and public key) are needed on the remote machine, however, only the public key file must be copied to the hub machine.

By default, the generated key's length is **2048** bits, and the private key is encrypted using **aes-256-cbc** algo rithm and the SSL certificate is signed using **sha256** hash algorithm. This can be customized by using the *o ptions* available for **hvrsslgen**.

Command argument *basename* is used for naming the key files. The private key file is named *basename***. priv_key** and the corresponding public key file is named *basename***.pub_cert**.

The second argument *subj* is written as plain text into the subject field of the X509 public certificate file and serves for reference purposes only. If argument *subj* contains two or more words with space between them, then it must be enclosed in double quotes. For example, "Certitficate for Cloud".

Options

This section describes the options available for command **hvrsslgen**.

Parameter	Description
-a*bits*	Generate an asymmetric (RSA) key pair with length *bits*. The **default** is **2048** bits.
-d*dir*	Generate files in directory *dir* instead of current directory.

-e*enc_alg*	Encrypt the private key using an internal password with encryption algorithm *enc_alg*. Valid values for *enc_alg* are: • **aes-128-cbc** • **aes-192-cbc** • **aes-256-cbc** (**default**) • **aes-128-cfb** • **aes-192-cfb** • **aes-256-cfb** • **aes-128-ecb** • **aes-192-ecb** • **aes-256-ecb** • **des-56-cbc** • **des-168-cbc**
-h*hash_alg*	Sign the SSL certificate using hash algorithm *hash_alg*. Valid values for *hash_alg* are: • **sha1** • **sha256** (**default**) • **sha512** • **md5**

Example

Run the following command to generate the private key and public certificate key pair:

```
hvrsslgen -a2048 -eaes-256-cfb -hsha512 MyCertificate "Certificate for Cloud"
```

The output will be as follows:

```
hvrsslgen: Generating SSL key pair...
hvrsslgen: Generating SSL key pair... completed.
hvrsslgen: Private key written to 'MyCertificate.priv_key'.
hvrsslgen: Public Certificate written to 'MyCertificate.pub_cert'.
hvrsslgen: Certificate subject: 'HVR Certificate for Cloud'
hvrsslgen: Certificate contains 2048 bit RSA Public Key.
hvrsslgen: Certificate valid from Nov  4 10:11:57 2015 GMT
hvrsslgen: Certificate valid until Oct 30 10:11:57 2035 GMT
hvrsslgen: Finished. (elapsed=1.85s)
```