Hvrproxy

Contents

Name

hvrproxy - HVR proxy.

Synopsis

hvrproxy [*-options*] *portnum access_conf.xml*

Description

HVR Proxy listens on a TCP/IP port number and invokes an **hvr** process with option **-x** (proxy mode) for each connection. The mechanism is the same as that of configuring an HVR proxy with the Unix daemon **inetd**.

On Windows, HVR Proxy is a Windows Service which is administered with option **-a**. The account under which it is installed must be member of the Administrator group, and must be granted privilege to act as part of the Operating System (**SeTcbPrivilege**). The service can either run as the default system account, or (if option **-P** is used) can run under the HVR account which created the Windows Service.

On Unix and Linux, HVR Proxy runs as a daemon which can be started with option **-d** and killed with option **-k**.

After the port number *portnum* an access configuration file *access_conf.xml* must be specified. This file is used to authenticate the identity of incoming connections and to control the outgoing connections. If the access file is a relative pathname, then it should be located in **$HVR_HOME/lib**.

⚠️ HVR Proxy is supported on Unix and Linux but it is more common on these machines to configure proxies using the **inetd** process to call executable **hvr** with options **-a** (access control file) and **-x** (proxy mode).
- When running as a Windows service, errors are written to the Windows event logs (**Control Panel Adminitrative Tools Event Viewer Windows Logs Application**).

Options

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

Parameter	Description

-a*x* **Windows**	Administration operations for Microsoft Windows system service. Values of *x* can be: • **c** : Create the HVR Proxy system service. • **s** : Start the HVR Proxy system service. • **h** : Halt (stop) the system service. • **d** : Destroy the system service. Several **-a***x* operations can be supplied together; allowed combinations are e.g. **-acs** (create and start) or **-ahd** (halt and destroy). HVR Proxy system service can be started (**-as**) and halted (**-ah**) from Windows Services (**Control Panel Administrative Tools Computer Management Services and Applications Services**).
-c*clus\clusgrp* **Windows**	Enroll the HVR Proxy service in a Windows cluster named *clus* in the cluster group *clusgrp*. Once the service is enrolled in the cluster it should only be stopped and started with the Windows cluster dialogs instead of the service being stopped and started directly (in the Windows Services dialog or with options **-as** or **-ah**). In Windows, failover clusters *clusgrp* is the network name of the item under **Services and Applications**. The group chosen should also contain the remote location; either the DBMS service for the remote database or the shared storage for a file location's top directory and state directory. The service needs to be created (with option **-ac**) on each node in the cluster. This service will act as a 'Generic Service' resource within the cluster. This option must be used with option **-a**.
-d	Start **hvrproxy** as a daemon process.
-E*name=value*	Set environment variable *name* to value *value* for the HVR processes started by this service.
-i	Interactive invocation. HVR Proxy stays attached to the terminal instead of redirecting its output to a log file.
-k	Stop **hvrproxy** daemon using the process-id in **$HVR_CONFIG/files/hvrproxy***port*.**pid**.
-K*pair*	SSL encryption using two files (public certificate and private key) to match public certificate supplied by **/SslRemoteCertificate**. If *pair* is relative, then it is found in directory **$HVR_HOME/lib/cert**. Value *pair* specifies two files; the names of these files are calculated by removing any extension from *pair* and then adding extensions **.pub_cert** and **.priv_key**. For example, option **-Khvr** refers to files **$HVR_HOME/lib/cert/hvr.pub_cert** and **$HVR_HOME/lib/cert/hvr.priv_key.**
-P*pwd* **Windows**	Configure HVR Proxy service to run under the current login HVR account using password *pwd*, instead of under the default system login account. May only be supplied with option **-ac**. Empty passwords are not allowed. The password is kept (hidden) within the Microsoft Windows OS and must be re-entered if passwords change.

Examples

The following access control file will restrict access to only connections from a certain network and to a pair of hosts.

```
<hvraccess>
  <allow>
    <from>
      <network>123.123.123.123/4</network>  <ssl remote_cert="cloud"/>
    </from>
    <to> <host>server1.internal</host> <port>4343</port> </to>
    <to> <host>server2.internal</host> <port>4343</port> </to>
  </allow>
</hvraccess>
```

If this XML is written to the default directory **$HVR_HOME/lib**, then a relative pathname can be used (e.g. **h vrproxy.xml**).

To create and start a Windows proxy service to listen on port number 4343:

```
c:\> hvrproxy -acs -Kproxy 4343 hvrproxy.xml
```

To configure an HVR proxy on Unix, add the following line to the **xinetd** configuration.

```
server_args= -x -Kproxy -ahvrproxy.xml
```

This connection can be tested with the following command:

```
$ hvrtestlistener -Kcloud -Cproxy -Rproxy-host:4343 server1.internal 4343
```

Files

HVR_HOME
  bin
    hvr — Executable for remote HVR service.
    hvrproxy — HVR Proxy executable.
  lib
    hvrproxy_example.xml — Sample proxy access file.

HVR_CONFIG
  files
    hvrproxy_port_**.pid** — Process-id of daemon started with option **-d**.
  log
    hvrproxy
      hvrproxy_port_**.log** — Logfile for daemon started with **-d**.

See Also

Command Hvr.