NAME

vnc.conf – configuration file for Virtual Network Computing

SYNOPSIS

$variable = "*someValue*";

$variable = "*someValue*";

$variable .= "*someValue*";

$variable = *$var1* . *$var2*;

DESCRIPTION

/etc/vnc.conf is the site wide configuration file for **tigervncserver**(1), the free X server for **Virtual Network Computing** (VNC). It can be used to change the behavior of the server at startup time, although for all values suitable defaults are preset.

vnc.conf will be parsed by tigervncserver. Then tigervncserver will proceed and read *$HOME/.vnc/vnc.conf*, a file that can be changed on a per-user base. It has the some syntax and options as the file described in this document.

EXAMPLES

The site wide configuration file */etc/vnc.conf* should come with the Debian package tigervnc-standalone-server. This file serves as an example for the user file *$HOME/.vnc/vnc.conf*. The site wide configuration file is pretty self-descriptive, and this document will mainly repeat the information that already can be found there.

OVERVIEW

The file is in **perl**(1) syntax, although only variable assignment is allowed for your safety and convenience. But there still a variety of possibilities to set the string variables.

All variable names are prefixed by '$'. You can assign a string to a variable using the '=' operator, and you can append a string to a variable using the '.=' operator. You can concatenate two strings using the '.' operator. You can substitute variables even inside quotes. You can access the environment variables using the notation *$ENV{VARIABLE}*.

You can unset a variable by assigning **undef** to it. Use this to return the state of the variable from 'set' to 'use default'.

You must end a line with a semicolon.

OPTIONS

The options are given with their default value if this is known.

$vncClasses = "*/var/www/vnc*";

Should be the path to the java classes of the server.

$baseHttpPort = *undef*;

This is the port base for the mini-HTTP server that is built-in to **Xtigervnc**(1)**.** The real http port will be derived from this base plus the display number.

$XFConfigPath = "*/etc/X11/xorg.conf*";

Can be set to the global *xorg.conf* file. This will be parsed to gain default values for *$fontPath*. If you want to disable this feature, point it to an invalid file, */invalid* for example.

$fontPath

Should be a comma separated list of fonts to be added to the font path. If not specified, and *$XFConfigPath* is valid, tigervncserver will read the $fontPath from there. If both are not set, the default will apply.

$PAMService = "tigervnc";

This parameter specifies the PAM service used for plain password authentication if one of the security types **Plain**, **TLSPlain**, or **X509Plain** is used. If */etc/pam.d/vnc* is not present, then **tigervncserver**(1) expects to use the **tigervnc** PAM service to authenticate the passwords of users when any of the ***Plain** security types are used. Note that the tigervnc-common package provides the PAM service configuration file */etc/pam.d/tigervnc*. Otherwise, if */etc/pam.d/vnc* is present, then the **vnc** PAM service will be used.

$sslAutoGenCertCommand = "openssl req
−newkey ec:/etc/tigervnc/ecparams.pem
−x509 −days 2190 −nodes";

The command specified by the *$sslAutoGenCertCommand* parameter is used to auto generate the certificate for the *−X509Cert* and *−X509Key* options of **Xtigervnc**(1)**.** The configuration for **openssl**(1SSL) is taken from */etc/tigervnc/ssleay.cnf* where we substitute **@HostName@** by the fully qualified domain name of the host.

$vncUserDir = "$ENV{HOME}/.vnc";

Contains the filename for the log files directory of Xtigervnc (the server) and the viewers that are connected to it.

$vncPasswdFile = $vncUserDir . "/passwd";

Contains the filename of the password file for Xtigervnc. This file is only used for the security types **VncAuth**, **TLSVnc**, and **X509Vnc**.

$vncStartup = "/etc/X11/XSession";

Points to a script that will be started at the very beginning of the Xtigervnc session.

$xauthorityFile = "$ENV{HOME}/.Xauthority";

Specifies the path to the X authority file that should be used by your Xtigervnc server.

$desktopName = "${HOSTFQDN}:nn ($ENV{LOGNAME})";

Should be set to the default name of the desktop. This can be changed at the command line with *-name*.

$wmDecoration = "8x64";

Sets the adjustment of *$geometry* to accommodate the window decoration used by the X11 window manager. This is used to fully display the VNC desktop even if the VNC viewer is not in full screen mode.

$geometry = "1900x1200";

This sets the framebuffer width & height. A default for this option as well as the *$depth* and *$pixelformat* options can be derived if the **tigervncserver**(1) is run in a X session – either $ENV{DISPLAY} or the session given by *$getDefaultFrom* – with the *−xdisplaydefaults* option. The geometry can also be changed at the commandline with the *−geometry* option. Otherwise, the fixed defaults given here as well as in the following two configuration parameter documentations will be used.

$depth = "32";

This sets the framebuffer color depth, i.e., the number of bits per pixel to use. It must be either 32, 24, 16, or 8.

$pixelformat = "rgb888";

Specifies the pixel format for the **Xtigervnc**(1) server to use (BGRnnn or RGBnnn). The default for depth 8 is BGR233 (meaning the most significant two bits represent blue, the next three green, and the least significant three represent red), the default for depth 16 is RGB565 and for depth 24 and 32 is RGB888.

$getDefaultFrom

This option lets you set the display from which you can query the default of the above three options, if you don't want to start tigervncserver from within a running X server. It will be added to the call of xdpyinfo. It is useful to get the default from the X server you will run xvncviewer in, because the data has not to be recalculated then.

$getDefaultFrom = "*−display localhost:0*"; is an example how to do this.

$rfbwait = "*30000*";

Sets the maximum time in msec to wait for the VNC client viewer.

$localhost = "*yes*";

Should the TigerVNC server only listen on localhost for incoming TigerVNC connections. This is useful if you use SSH and want to stop non-SSH connections from any other hosts. Hence, *$localhost* = "*yes*" is the default if security types are not specified. In this case, only the security type **VncAuth** will be offered. If the security types are specified, either via the option *−SecurityTypes* given to **tigervncserver**(1) or via the *$SecurityTypes* configuration parameter in */etc/vnc.conf* or in *$HOME/.vnc/vnc.conf*, then the default depends on the specified security types. The default will be *$localhost* = "*no*" if the specified security types contain at least one of the **TLS*** or **X509*** secutity types and also contain none of the ***None** security types. As always, the defaults can be overwritten on the commandline via the *−localhost* option or via the *$localhost* configuration parameter in */etc/vnc.conf* or in *$HOME/.vnc/vnc.conf*.

$SecurityTypes = "**VncAuth**"

The *$SecurityTypes* parameter contains a comma separated list of the default security types the Xtigervnc server will offer. Available security types are **None**, **VncAuth**, **Plain**, **TLSNone**, **TLSVnc**, **TLSPlain**, **X509None**, **X509Vnc** and **X509Plain**. The ***None** security types do not offer any kind of user authentication for connecting VNC sessions. Hence, combining a ***None** security type and *$localhost* = "*no*" is a very bad idea. The **TLS*** and **X509*** security types do enforce SSL encryption for data transmission. Hence, combining a **TLS*** or **X509*** security type and *$localhost* = "*yes*" is a senseless idea. Thus, in the case of *$localhost* = "*no*", the default for *$SecurityTypes* will be extended from **VncAuth** to **VncAuth**,**TLSVnc**.

$PlainUsers = "*$ENV{LOGNAME}*"

The *$PlainUsers* configuration parameter contains a comma separated list of users that are authorized to access the VNC server if the security types **Plain**, **TLSPlain**, or **X509Plain** are used to establish the connection. The password for these users are check by the system via the PAM service specified via *$PAMService* option. On default, only the user starting the tigervncserver is contained in the list. By specifying *, any user can authenticate using this security type.

$X509Cert and *$X509Key*

These two options contain the filenames for a certificate and its key that is used for the security types **X509None**, **X509Vnc**, and **X509Plain**. If nothing is specified – the default case – then a self-signed certificate is auto-generated by **tigervncserver**(1) and stored in *$HOME/.vnc/${HOSTFQDN}-SrvCert.pem* and *$HOME/.vnc/${HOSTFQDN}-SrvKey.pem*, respectively. If filenames are given for *$X509Cert* and *$X509Key* either here or on the commandline via *−X509Cert* and *−X509Key* options, then the auto generation is disabled and the user has to take care that usable certificates are present.

FILES

/usr/bin/tigervncserver

A wrapper script around **Xtigervnc** to start the server with appropriate defaults.

/usr/bin/tigervncpasswd

Command to create and change password files to be used by the RFB protocol (can be specified in the *$vncPasswdFile* variable). **/usr/bin/Xtigervnc** The real server. Will be invoked by tigervncserver.

SEE ALSO

Xtigervnc(1), **tigervncserver**(1), **x0tigervncserver**(1), **tigervncpasswd**(1), **xtigervncviewer**(1).

AUTHOR

2016 – Modified for TigerVNC 1.7 by Joachim Falk (Joachim.falk@gmx.de) 2006 – Modified for vnc 4.1.2 by Joachim Falk (Joachim.falk@gmx.de) 1998 – Originally written by Marcus Brinkmann (Marcus.Brinkmann@ruhr-uni-bochum.de) for the Debian GNU/Linux Distribution.