Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'cockpit.conf.5' command

$ man cockpit.conf.5

COCKPIT.CONF(5) cockpit.conf COCKPIT.CONF(5)

NAME

cockpit.conf - Cockpit configuration file

DESCRIPTION

Cockpit can be configured via /etc/cockpit/cockpit.conf. This file is not required and may need to be created manually. The file has a INI file syntax and thus contains key / value pairs, grouped into topical groups. See the examples below for details..

Note: The port that cockpit listens on cannot be changed in this file. To change the port change the systemd cockpit.socket file.

WEBSERVICE

Origins

By default cockpit will not accept crossdomain websocket connections. Use this setting to allow access from alternate domains. Origins should include scheme, host and port, if necessary.

[WebService]

Origins = https://somedomain1.com https://somedomain2.com:9090

ProtocolHeader

Configure cockpit to look at the contents of this header to determine if a connection is using tls. This should only be used when cockpit is behind a reverse proxy, and care should be taken to make sure that incoming requests cannot set this header.

[WebService]

ProtocolHeader = X-Forwarded-Proto

ForwardedForHeader

Configure cockpit to look at the contents of this header to determine the real origin of a connection. This should only be used when cockpit is behind a reverse proxy, and care should be taken to make sure that incoming requests cannot set this header.

[WebService]

ForwardedForHeader = X-Forwarded-For

LoginTitle

Set the browser title for the login screen.

LoginTo

When set to true the Connect to option on the login screen is visible and allows logging into another server. If this option is not specified then it will be automatically detected based on whether the cockpit-ssh process is available or not.

RequireHost

When set to true cockpit will require users to use the Connect to option to specify the host to log into.

MaxStartups

Same as the sshd configuration option by the same name. Specifies the maximum number of concurrent login attempts allowed. Additional connections will be dropped until authentication succeeds or the connections are closed. Defaults to 10.

Alternatively, random early drop can be enabled by specifying the three colon separated values start:rate:full (e.g. "10:30:60"). Cockpit will start refusing authentication attempts with a probability of rate/100 (30%) if there are currently start (10) unauthenticated connections. The probability increases linearly and all connection attempts are refused if the number of unauthenticated connections reaches full (60).

AllowUnencrypted

If true, cockpit will accept unencrypted HTTP connections.

Otherwise, it redirects all HTTP connections to HTTPS. Exceptions are connections from localhost and for certain URLs (like /ping). Defaults to false.

UrlRoot

The root URL where you will be serving cockpit. When provided cockpit will expect all requests to be prefixed with the given url. This is mostly useful when you are using cockpit behind a reverse proxy, such as nginx. /cockpit/ and /cockpit+ are reserved and should not be used. For example /cockpit-new/ is ok. /cockpit/ and /cockpit+new/ are not.

ClientCertAuthentication

If true, enable TLS client certificates for authenticating users. Commonly these are provided by a smart card, but it's equally possible to import certificates directly into the web browser. Please see the Certificate/smart card authentication[1] section in the Cockpit guide for details.

Shell

The relative URL to top level component to display in Cockpit once logged in. Defaults to /shell/index.html

LOG

Fatal

The kind of log messages in the bridge to treat as fatal. Separate multiple values with spaces. Relevant values are: criticals and warnings.

OAUTH

Cockpit can be configured to support the implicit grant[2] OAuth authorization flow. When successful the resulting oauth token will be passed to cockpit-ws using the Bearer auth-scheme. For a login to be successful, cockpit will also need a to be configured to verify and allow Bearer tokens.

URL

This is the url that cockpit will redirect the users browser to when it needs to obtain an oauth token. Cockpit will add a

redirect_uri parameter to the url with the location of where the oauth provider should redirect to once a token has been obtained.

ErrorParam

When a oauth provider redirects a user back to cockpit, look for this parameter in the querystring or fragment portion of the url to find a error message. When not provided it will default to error_description

TokenParam

When a oauth provider redirects a user back to cockpit, look for this parameter in the querystring or fragment portion of the url to find the access token. When not provided it will default to access_token

SESSION

Banner

The contents of the specified file (commonly /etc/issue) are shown on the login page. By default, no banner is displayed.

IdleTimeout

Time in minutes after which session expires and user is logged out if no user action has been performed in the given time. This idle timeout only applies to interactive password logins. With non-interactive authentication methods like Kerberos, OAuth, or certificate login, the browser cannot forget credentials, and thus automatic logouts are not useful for protecting credentials of forgotten sessions. Set to 0 to disable session timeout.

```
[Session]
IdleTimeout=15
```

When not specified, there is no idle timeout by default.

BUGS

Please send bug reports to either the distribution bug tracker or the upstream bug tracker[3].

AUTHOR

Cockpit has been written by many contributors[4].

SEE ALSO

cockpit-ws(8), cockpit-tls(8)

NOTES

1. Certificate/smart card authentication

   https://cockpit-project.org/guide/latest/cert-authentication.html

2. implicit grant

   https://tools.ietf.org/html/rfc6749#section-4.2

3. upstream bug tracker

   https://github.com/cockpit-project/cockpit/issues/new

4. contributors

   https://github.com/cockpit-project/cockpit/