Item 186
git_comments:

1. Replace the password with a copy of the string after "file:"
2. skip the "pass:" header
3. If the password starts with a file: literal set the is_file to true.
4. The global variable errno (found in <errno.h>) contains information about what went wrong; you can use perror() to print that information as a readable string
5. Warn the user that the passwordFile attribute has been deprecated.
6. Replace the password with a copy of the string after "literal: or "pass:"
7. If the "password" starts with "literal:" or "pass:" then
8. * * Read the file from the password_file location on the file system and populate password_field with the * contents of the file.
9. THe password field does not have any prefixes. Use it as plain text

git_commits:

1. **summary:** DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and modified the password field to accept openssl style prefixes. This closes #582.
   message: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and modified the password field to accept openssl style prefixes. This closes #582.

github_issues:

github_issues_comments:

github_pulls:

1. **title:** DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m…
   body: …odified the password field to accept openssl style prefixes

github_pulls_comments:

1. # [Codecov](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=h1) Report > Merging [#582](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=desc) into [master] (https://codecov.io/gh/apache/qpid-dispatch/commit/366c6e61a299a6a672b6ea81974d96f465499e71? src=pr&el=desc) will **increase** coverage by `0.01%`. > The diff coverage is `93.18%`. [![Impacted file tree graph](https://codecov.io/gh/apache/qpid-dispatch/pull/582/graphs/tree.svg? width=650&token=rk2Cgd27pP&height=150&src=pr)](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=tree) ```diff @@ Coverage Diff @@ ## master #582 +/- ## === + Coverage 86.3% 86.31% +0.01% === Files 90 90 Lines 20388 20404 +16 === + Hits 17595 17611 +16 Misses 2793 2793 ``` | [Impacted Files](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=tree) | Coverage Δ | | |--- -|---|---| | [src/connection_manager.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff? src=pr&el=tree#diff-c3JjL2Nvbm5lY3Rpb25fbWFuYWdlci5j) | `91.3% <93.18%> (+1.73%)` | :arrow_up: | | [src/router_core/transfer.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff? src=pr&el=tree#diff-c3JjL3JvdXRlcl9jb3JlL3RyYW5zZmVyLmM=) | `93.51% <0%> (-1%)` | :arrow_down: | | [src/router_core/agent_link.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff? src=pr&el=tree#diff-c3JjL3JvdXRlcl9jb3JlL2FnZW50X2xpbmsuYw==) | `66.83% <0%> (-0.51%)` | :arrow_down: | | [src/router_core/route_tables.c](https://codecov.io/gh/apache/qpid- dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3JvdXRlcl9jb3JlL3JvdXRlX3RhYmxlcy5j) | `75.68% <0%> (-0.5%)` | :arrow_down: | | [src/router_node.c](https://codecov.io/gh/apache/qpid- dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3JvdXRlcl9ub2RlLmM=) | `92.88% <0%> (-0.25%)` | :arrow_down: | | [src/iterator.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff? src=pr&el=tree#diff-c3JjL2l0ZXJhdG9yLmM=) | `89.34% <0%> (-0.02%)` | :arrow_down: | | [src/router_core/router_core.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff? src=pr&el=tree#diff-c3JjL3JvdXRlcl9jb3JlL3JvdXRlcl9jb3JlLmM=) | `86.73% <0%> (+0.19%)` | :arrow_up: | | [src/parse.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-

2. @bhardesty @kgiusti I think I have addressed your comments. Please take a look at the PR once again and approve if satisfied. Thanks.

github_pulls_reviews:

1. I know it's not obvious, but this file is an old version that is no longer published as part of the user guide. Instead of one, generic procedure for configuring an sslProfile, it's now included within the procedures for each scenario in which you would use an sslProfile (each of which would probably require a different sslProfile to be configured): Connecting routers together (i.e. inter-router): https://qpid.apache.org/releases/qpid-dispatch-1.9.0/user-guide/index.html#securing-connections-between-routers-router Enabling encryption/authentication for incoming "normal" connections: https://qpid.apache.org/releases/qpid-dispatch-1.9.0/user-guide/index.html#enabling-ssl-tls-encryption-router Connecting securely to an external container with mutual TLS: https://qpid.apache.org/releases/qpid-dispatch-1.9.0/user-guide/index.html#connecting-using-mutual-ssl-tls-authentication-router Connecting securely to an external container with one-way TLS: https://qpid.apache.org/releases/qpid-dispatch-1.9.0/user-guide/index.html#connecting-using-one-way-ssl-tls-authentication-router For each of these instances of sslProfile, if appropriate to the scenario at hand, I would add the "password" attribute.
2. What happens when the fopen fails, like read permission or file not found? This looks as if we fail silently. We need a log error here.
3. passwrod?
4. I wouldn't mention openssl here - we're not exactly compatible due to "literal:"
5. **body:** I'd recommend including the output of "strerror(errno)" in the log file and remove the perror stuff (no stderr if in daemon mode): qd_log(log_source, QD_LOG_WARNING, "Unable to open password file %s, error: %s", password_file, strerror(errno));
   label: code-design
6. It's only a file if the password text includes the "file:" prefix, correct?
7. Also needs "file:" prefix
8. Remove "openssl" and fix "passwrod"
9. Oh, and make the log level error.

jira_issues:

1. **summary:** Deprecate the passwordFile field in sslProfile and consolidate all password scenarios to use the password field
   description: Deprecate the passwordFile field and consolidate all password scenarios to use the password field. We will use the password options that [openssl|https://www.openssl.org/docs/man1.1.1/man1/openssl.html] uses (see Pass Phrase Options sections). Going forward, here are three ways to specify a password in an sslProfile   {noformat} sslProfile {   caCertFile: .....   certFile: .....   # Get the password from the environment variable TLS_SERVER_PASSWORD. Note the env: prefix   password: env:TLS_SERVER_PASSWORD OR   # Get the password from the absolute file path. Note the file: prefix   password: file:/home/tls/password-file.txt   OR   # Specify the actual password. Note the pass: prefix password: pass:actual_password } {noformat} (We will not be supporting the openssl options fd: and stdin   While you can still specify the actual password in the password field using the pass: prefix, which casual users might want to do, you are also able to specify the file path or environment variable for more robust security. This change will be backward compatible which means, you will still be able to specify the actual password in the password field without the pass: prefix. The "literal" prefix will continue to work as well. The passwordFile field will be deprecated and eventually removed when we to a major version.

jira_issues_comments:

1. ganeshmurthy commented on pull request #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582 …odified the password field to accept openssl style prefixes -- This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org

2. codecov-io commented on issue #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582#issuecomment-539095930 # [Codecov](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=h1) Report > Merging [#582](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=desc) into [master](https://codecov.io/gh/apache/qpid-dispatch/commit/366c6e61a299a6a672b6ea81974d96f465499e71?src=pr&el=desc) will **increase** coverage by `0.02%`. > The diff coverage is `100%`. [![Impacted file tree graph](https://codecov.io/gh/apache/qpid-dispatch/pull/582/graphs/tree.svg?width=650&token=rk2Cgd27pP&height=150&src=pr)](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=tree) ```diff @@ Coverage Diff @@ ## master #582 +/- ## == + Coverage 86.3% 86.32% +0.02% == Files 90 90 Lines 20388 20402 +14 == + Hits 17595 17612 +17 + Misses 2793 2790 -3 ``` | [Impacted Files](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=tree) | Coverage Δ | | |---|---|---| | [src/connection_manager.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL2Nvbm5lY3Rpb25fbWFuYWdlci5j) | `91.84% <100%> (+2.27%)` | :arrow_up: | | [src/router_core/agent_link.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3JvdXRlcl9jb3JlL2FnZW50X2xpbmsuYw==) | `66.83% <0%> (-0.51%)` | :arrow_down: | | [src/router_core/transfer.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3JvdXRlcl9jb3JlL3RyYW5zZmVyLmM=) | `94.01% <0%> (-0.5%)` | :arrow_down: | | [src/router_core/route_tables.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3JvdXRlcl9jb3JlL3JvdXRlX3RhYmxlcy5j) | `75.68% <0%> (-0.5%)` | :arrow_down: | | [src/router_node.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3JvdXRlcl9ub2RlLmM=) | `92.88% <0%> (-0.25%)` | :arrow_down: | | [src/router_core/connections.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3JvdXRlcl9jb3JlL2Nvbm5lY3Rpb25zLmM=) | `93.86% <0%> (-0.23%)` | :arrow_down: | | [src/iterator.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL2l0ZXJhdG9yLmM=) | `89.17% <0%> (-0.19%)` | :arrow_down: | | [src/container.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL2NvbnRhaW5lci5j) | `81.37% <0%> (+0.18%)` | :arrow_up: | | [src/router_core/router_core.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3JvdXRlcl9jb3JlL3JvdXRlcl9jb3JlLmM=) | `86.73% <0%> (+0.19%)` | :arrow_up: | | [src/parse.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3BhcnNlLmM=) | `87.86% <0%> (+0.22%)` | :arrow_up: | | ... and [1 more](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree-more) | | ------ [Continue to review full report at Codecov](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=continue). > **Legend** - [Click here to learn more](https://docs.codecov.io/docs/codecov-delta) > `Δ = absolute <relative> (impact)`, `ø = not affected`, `? = missing data` > Powered by [Codecov](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=footer). Last update [366c6e6...ce2f1ac](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=lastupdated). Read the [comment docs](https://docs.codecov.io/docs/pull-request-comments). -- This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org

3. bhardesty commented on pull request #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582#discussion_r332134469 ########## File path: docs/books/user-guide/configuration-security.adoc ########## @@ -133,7 +133,7 @@ For example: privateKeyFile: /qdrouterd/ssl_certs/router-key-pwd.pem ---- -`passwordFile` or `password`:: If the private key is password-protected, you must provide the password by either specifying the absolute path to a file containing the password that unlocks the certificate key, or entering the password directly in the configuration file. +`passwordFile` or `password`:: If the private key is password-protected, you must provide the password by either specifying the absolute path to a file containing the password that unlocks the certificate key, or entering the password directly in the configuration file. Entering the password directly in the configuration file is unsafe. passwordFile has

been deprecated. Use password. Review comment: I know it's not obvious, but this file is an old version that is no longer published as part of the user guide. Instead of one, generic procedure for configuring an sslProfile, it's now included within the procedures for each scenario in which you would use an sslProfile (each of which would probably require a different sslProfile to be configured): Connecting routers together (i.e. inter-router): https://qpid.apache.org/releases/qpid-dispatch-1.9.0/user-guide/index.html#securing-connections-between-routers-router Enabling encryption/authentication for incoming "normal" connections: https://qpid.apache.org/releases/qpid-dispatch-1.9.0/user-guide/index.html#enabling-ssl-tls-encryption-router Connecting securely to an external container with mutual TLS: https://qpid.apache.org/releases/qpid-dispatch-1.9.0/user-guide/index.html#connecting-using-mutual-ssl-tls-authentication-router Connecting securely to an external container with one-way TLS: https://qpid.apache.org/releases/qpid-dispatch-1.9.0/user-guide/index.html#connecting-using-one-way-ssl-tls-authentication-router For each of these instances of sslProfile, if appropriate to the scenario at hand, I would add the "password" attribute. -- This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org

4. kgiusti commented on pull request #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582#discussion_r332157060 ########## File path: docs/books/user-guide/configuration-reference.adoc ########## @@ -76,8 +76,8 @@ Attributes for setting SSL/TLS configuration for connections. * *_caCertFile_* (path) : The absolute path to the database that contains the public certificates of trusted certificate authorities (CA). * *_certFile_* (path) : The absolute path to the file containing the PEM-formatted public certificate to be used on the local end of any connections using this profile. * *_privateKeyFile_* (path) : The absolute path to the file containing the PEM-formatted private key for the above certificate. -* *_passwordFile_* (path) : If the above private key is password protected, this is the absolute path to a file containing the password that unlocks the certificate key. -* *_password_* (string) : An alternative to storing the password in a file referenced by passwordFile is to supply the password right here in the configuration file. This option can be used by supplying the password in the 'password' option. Don't use both password and passwordFile in the same profile. +* *_passwordFile_* (path) : (DEPRECATED) If the above private key is password protected, this is the absolute path to the file containing the password that unlocks the certificate key. This file should be permission protected to limit access. This has been deprecated. Use the file: prefix in the password field to specify the absolute path of the file containing the password. If both password and passwordFile are provided, the passwordFile is ignored. +* *_password_* (string) : Password that unlocks the certificate key. Supports three openssl style prefixes namely - env:, file: pass:. Also supports the legacy literal: prefix. env:var obtains the password from the environment variable var. Since the environment of other processes is visible on certain platforms (e.g. ps under certain Unix OSes) this option should be used with caution. file:absolutepath obtains passswrod from the absolute path of the file containing the password. This option is the safest since permissions can be set on the file. pass:password or literal:password or password with no prefix is used to directly specify the password and should only be used where security is not important. If both password and passwordFile are provided, the passwordFile is ignored. Review comment: passwrod? --- This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org

5. kgiusti commented on pull request #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582#discussion_r332156779 ########## File path: src/connection_manager.c ########## @@ -103,6 +103,38 @@ static qd_config_ssl_profile_t *qd_find_ssl_profile(qd_connection_manager_t *cm, return 0; } +/** + * Read the file from the password_file location on the file system and populate password_field with the + * contents of the file. + */ +static void qd_set_password_from_file(char *password_file, char **password_field) +{ + if (password_file) { + FILE *file = fopen(password_file, "r"); Review comment: What happens when the fopen fails, like read permission or file not found? This looks as if we fail silently. We need a log error here. -- This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org

6. kgiusti commented on pull request #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582#discussion_r332160677 ########## File path: python/qpid_dispatch/management/qdrouter.json ########## @@ -633,14

+633,14 @@ }, "passwordFile": { "type": "path", - "description": "If the above private key is password protected, this is the absolute path to a file containing the password that unlocks the certificate key. This file should be permission protected to limit access", + "description": "(DEPRECATED) If the above private key is password protected, this is the absolute path to the file containing the password that unlocks the certificate key. This file should be permission protected to limit access. This has been deprecated. Use the file: prefix in the password field to specify the absolute path of the file containing the password. If both password and passwordFile are provided, the passwordFile is ignored", + "deprecated": true, "create": true }, "password": { "type": "string", - "description": "(DEPRECATED) An alternative to storing the password in a file referenced by passwordFile is to supply the password right here in the configuration file. This takes precedence over the passwordFile if both are specified. This attribute has been deprecated because it is unsafe to store plain text passwords in config files. Use the passwordFile instead", - "deprecated": true, + "description": "Password that unlocks the certificate key. Supports three openssl style prefixes namely - env:, file: pass:. Also supports the legacy literal: prefix. env:var obtains the password from the environment variable var. Since the environment of other processes is visible on certain platforms (e.g. ps under certain Unix OSes) this option should be used with caution. file:absolutepath obtains the password from the absolute path of the file containing the password. This option is the safest since permissions can be set on the file. pass:password or literal:password or password with no prefix is used to directly specify the password and should only be used where security is not important. If both password and passwordFile are provided, the passwordFile is ignored", Review comment: I wouldn't mention openssl here - we're not exactly compatible due to "literal:" -- This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org

7. ganeshmurthy commented on issue #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582#issuecomment-539167128 @bhardesty @kgiusti I think I have addressed your comments. Please take a look at the PR once again and approve if satisfied. Thanks. -- This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org

8. codecov-io commented on issue #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582#issuecomment-539095930 # [Codecov](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=h1) Report > Merging [#582](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=desc) into [master](https://codecov.io/gh/apache/qpid-dispatch/commit/366c6e61a299a6a672b6ea81974d96f465499e71?src=pr&el=desc) will **increase** coverage by `0.01%`. > The diff coverage is `93.18%`. [![Impacted file tree graph](https://codecov.io/gh/apache/qpid-dispatch/pull/582/graphs/tree.svg?width=650&token=rk2Cgd27pP&height=150&src=pr)](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=tree) ```diff @@ Coverage Diff @@ ## master #582 +/- ## === + Coverage 86.3% 86.31% +0.01% === Files 90 90 Lines 20388 20404 +16 === + Hits 17595 17611 +16 Misses 2793 2793 ``` | [Impacted Files](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=tree) | Coverage Δ | | |---|---|---| | [src/connection_manager.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL2Nvbm5lY3Rpb25fbWFuYWdlci5j) | `91.3% <93.18%> (+1.73%)` | :arrow_up: | | [src/router_core/transfer.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3JvdXRlcl9jb3JlL3RyYW5zZmVyLmM=) | `93.51% <0%> (-1%)` | :arrow_down: | | [src/router_core/agent_link.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3JvdXRlcl9jb3JlL2FnZW50X2xpbmsuYw==) | `66.83% <0%> (-0.51%)` | :arrow_down: | | [src/router_core/route_tables.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3JvdXRlcl9jb3JlL3JvdXRlX3RhYmxlcy5j) | `75.68% <0%> (-0.5%)` | :arrow_down: | | [src/router_node.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3JvdXRlcl9ub2RlLmM=) | `92.88% <0%> (-0.25%)` | :arrow_down: | | [src/iterator.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL2l0ZXJhdG9yLmM=) | `89.34% <0%> (-0.02%)` | :arrow_down: | | [src/router_core/router_core.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3JvdXRlcl9jb3JlL3JvdXRlcl9jb3JlLmM=) | `86.73% <0%> (+0.19%)` | :arrow_up: | | [src/parse.c](https://codecov.io/gh/apache/qpid-dispatch/pull/582/diff?src=pr&el=tree#diff-c3JjL3BhcnNlLmM=) | `87.86% <0%> (+0.22%)` | :arrow_up: | | ------ [Continue to review full report at

Codecov](https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=continue). > **Legend** - [Click here to learn more](https://docs.codecov.io/docs/codecov-delta) > `Δ = absolute <relative> (impact)`, `ø = not affected`, `? = missing data` > Powered by [Codecov] (https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=footer). Last update [366c6e6...03ea666] (https://codecov.io/gh/apache/qpid-dispatch/pull/582?src=pr&el=lastupdated). Read the [comment docs] (https://docs.codecov.io/docs/pull-request-comments). -- --- This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org

9. kgiusti commented on pull request #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582#discussion_r332507603 ########## File path: src/connection_manager.c ########## @@ -107,31 +107,39 @@ static qd_config_ssl_profile_t *qd_find_ssl_profile(qd_connection_manager_t *cm, * Read the file from the password_file location on the file system and populate password_field with the * contents of the file. */ - static void qd_set_password_from_file(char *password_file, char **password_field) +static void qd_set_password_from_file(char *password_file, char **password_field, qd_log_source_t *log_source) { if (password_file) { FILE *file = fopen(password_file, "r"); - if (file) { - char buffer[200]; + if (file == NULL) { + // + // The global variable errno (found in <errno.h>) contains information about what went wrong; you can use perror() to print that information as a readable string + // + qd_log(log_source, QD_LOG_WARNING, "Unable to open password file %s", password_file); Review comment: I'd recommend including the output of "strerror(errno)" in the log file and remove the perror stuff (no stderr if in daemon mode): qd_log(log_source, QD_LOG_WARNING, "Unable to open password file %s, error: %s", password_file, strerror(errno)); -- This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org

10. kgiusti commented on pull request #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582#discussion_r332511087 ########## File path: docs/books/user-guide/modules/connecting-using-mutual-ssl-tls-authentication.adoc ########## @@ -55,9 +55,11 @@ sslProfile { `certFile`:: The absolute path to the file containing the public certificate for this router. +`caCertFile`:: The absolute path to the CA certificate that was used to sign the router's certificate. + `privateKeyFile`:: The absolute path to the file containing the private key for this router's public certificate. -`caCertFile`:: The absolute path to the CA certificate that was used to sign the router's certificate. +`password`:: The absolute path to the file that contains the password to unlock the certificate key. Not specified if certificate key has no password. Review comment: It's only a file if the password text includes the "file:" prefix, correct? -- ---------------------- This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org

11. kgiusti commented on pull request #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582#discussion_r332511326 ########## File path: docs/books/user-guide/modules/enabling-ssl-tls-encryption.adoc ########## @@ -46,18 +46,21 @@ This `sslProfile` contains the locations of the private key and certificates tha sslProfile { name: service-tls certFile: /etc/qpid-dispatch-certs/normal/tls.crt - privateKeyFile: /etc/qpid-dispatch-certs/normal/tls.key caCertFile: /etc/qpid-dispatch-certs/client-ca/ca.crt + privateKeyFile: /etc/qpid-dispatch-certs/normal/tls.key + password: file:/etc/qpid-dispatch-certs/inter-router/password.txt ... } ---- `name`:: A unique name that you can use to refer to this `sslProfile`. `certFile`:: The absolute path to the file containing the public certificate for this router. +`caCertFile`:: The absolute path to the CA certificate that was used to sign the router's certificate. + `privateKeyFile`:: The absolute path to the file containing the private key for this router's public certificate. -`caCertFile`:: The absolute path to the CA certificate that was used to sign the router's certificate. +`password`:: The absolute path to the file that contains the password to unlock the certificate key. Not specified if certificate key has no password. Review comment: Also needs "file:" prefix -- ------ This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org

12. kgiusti commented on pull request #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582#discussion_r332512084 ########## File path: docs/books/user-guide/configuration-reference.adoc ########## @@ -76,8 +76,8

@@ Attributes for setting SSL/TLS configuration for connections. * *_caCertFile_* (path) : The absolute path to the database that contains the public certificates of trusted certificate authorities (CA). * *_certFile_* (path) : The absolute path to the file containing the PEM-formatted public certificate to be used on the local end of any connections using this profile. * *_privateKeyFile_* (path) : The absolute path to the file containing the PEM-formatted private key for the above certificate. -* *_passwordFile_* (path) : If the above private key is password protected, this is the absolute path to a file containing the password that unlocks the certificate key. -* *_password_* (string) : An alternative to storing the password in a file referenced by passwordFile is to supply the password right here in the configuration file. This option can be used by supplying the password in the 'password' option. Don't use both password and passwordFile in the same profile. +* *_passwordFile_* (path) : (DEPRECATED) If the above private key is password protected, this is the absolute path to the file containing the password that unlocks the certificate key. This file should be permission protected to limit access. This has been deprecated. Use the file: prefix in the password field to specify the absolute path of the file containing the password. If both password and passwordFile are provided, the passwordFile is ignored. +* *_password_* (string) : Password that unlocks the certificate key. Supports three openssl style prefixes namely - env:, file: pass:. Also supports the legacy literal: prefix. env:var obtains the password from the environment variable var. Since the environment of other processes is visible on certain platforms (e.g. ps under certain Unix OSes) this option should be used with caution. file:absolutepath obtains passswrod from the absolute path of the file containing the password. This option is the safest since permissions can be set on the file. pass:password or literal:password or password with no prefix is used to directly specify the password and should only be used where security is not important. If both password and passwordFile are provided, the passwordFile is ignored. Review comment: Remove "openssl" and fix "passwrod" --- This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org

13. kgiusti commented on pull request #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582#discussion_r332513289 ########## File path: src/connection_manager.c ########## @@ -107,31 +107,39 @@ static qd_config_ssl_profile_t *qd_find_ssl_profile(qd_connection_manager_t *cm, * Read the file from the password_file location on the file system and populate password_field with the * contents of the file. */ - static void qd_set_password_from_file(char *password_file, char **password_field) +static void qd_set_password_from_file(char *password_file, char **password_field, qd_log_source_t *log_source) { if (password_file) { FILE *file = fopen(password_file, "r"); - if (file) { - char buffer[200]; + if (file == NULL) { + // + // The global variable errno (found in <errno.h>) contains information about what went wrong; you can use perror() to print that information as a readable string + // + qd_log(log_source, QD_LOG_WARNING, "Unable to open password file %s", password_file); Review comment: Oh, and make the log level error. --- This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org

14. Commit 7bcd40aec8bb059e1ea200c7b126635ba0903139 in qpid-dispatch's branch refs/heads/master from Ganesh Murthy [https://gitbox.apache.org/repos/asf?p=qpid-dispatch.git;h=7bcd40a] DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and modified the password field to accept openssl style prefixes. This closes #582.

15. asfgit commented on pull request #582: DISPATCH-1440 - Deprecated passwordFile attribute in sslProfile and m… URL: https://github.com/apache/qpid-dispatch/pull/582 --- This is an automated message from the Apache Git Service. To respond to the message, please log on to GitHub and use the URL above to go to the specific comment. For queries about this service, please contact Infrastructure at: users@infra.apache.org