Ruby - Feature #14940

Support bcrypt password hashing in webrick

07/25/2018 11:36 PM - jeremyevans0 (Jeremy Evans)

Status:	Closed	
Priority:	Normal	
Assignee:	normalperson (Eric Wong)	
Target version:		

Description

Related to #14915, this adds bcrypt password hash support when using htpasswd files with Webrick basic auth, allowing a migration path away from the current String#crypt usage.

Related issues:

Related to Ruby - Feature #14915: Deprecate String#crypt	**Rejected**

Associated revisions

Revision 9749bfbf735f8dca3361f2ea16bb97027bd1ab61 - 07/26/2018 03:21 AM - Eric Wong

webrick: Support bcrypt password hashing

This adds a password_hash keyword argument to
WEBrick::HTTPAuth::Htpasswd#initialize. If set to :bcrypt, it
will create bcrypt hashes instead of crypt hashes, and will
raise an exception if the .htpasswd file uses crypt hashes.

If :bcrypt is used, then instead of calling
BasicAuth.make_passwd (which uses crypt),
WEBrick::HTTPAuth::Htpasswd#set_passwd will set the bcrypt
password directly. It isn't possible to change the
make_passwd API to accept the password hash format, as that
would break configurations who use Htpasswd#auth_type= to set
a custom auth_type.

This modifies WEBrick::HTTPAuth::BasicAuth to handle checking
both crypt and bcrypt hashes.

There are commented out requires for 'string/crypt', to handle
when String#crypt is deprecated and the undeprecated version is
moved to a gem.

There is also a commented out warning for the case when
the password_hash keyword is not specified and 'string/crypt'
cannot be required. I think the warning makes sense to nudge
users to using bcrypt.

I've updated the tests to test nil, :crypt, and :bcrypt values
for the password_hash keyword, skipping the bcrypt tests if the
bcrypt library cannot be required.

[ruby-core:88111] [Feature #14940]

From: Jeremy Evans code@jeremyevans.net

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@64060 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 9749bfbf735f8dca3361f2ea16bb97027bd1ab61 - 07/26/2018 03:21 AM - Eric Wong

webrick: Support bcrypt password hashing

This adds a password_hash keyword argument to
WEBrick::HTTPAuth::Htpasswd#initialize. If set to :bcrypt, it
will create bcrypt hashes instead of crypt hashes, and will
raise an exception if the .htpasswd file uses crypt hashes.

If :bcrypt is used, then instead of calling
BasicAuth.make_passwd (which uses crypt),
WEBrick::HTTPAuth::Htpasswd#set_passwd will set the bcrypt
password directly. It isn't possible to change the

make_passwd API to accept the password hash format, as that would break configurations who use Htpasswd#auth_type= to set a custom auth_type.

This modifies WEBrick::HTTPAuth::BasicAuth to handle checking both crypt and bcrypt hashes.

There are commented out requires for 'string/crypt', to handle when String#crypt is deprecated and the undeprecated version is moved to a gem.

There is also a commented out warning for the case when the password_hash keyword is not specified and 'string/crypt' cannot be required. I think the warning makes sense to nudge users to using bcrypt.

I've updated the tests to test nil, :crypt, and :bcrypt values for the password_hash keyword, skipping the bcrypt tests if the bcrypt library cannot be required.

[ruby-core:88111] [Feature #14940]

From: Jeremy Evans code@jeremyevans.net

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@64060 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 9749bfbf - 07/26/2018 03:21 AM - Eric Wong

webrick: Support bcrypt password hashing

This adds a password_hash keyword argument to WEBrick::HTTPAuth::Htpasswd#initialize. If set to :bcrypt, it will create bcrypt hashes instead of crypt hashes, and will raise an exception if the .htpasswd file uses crypt hashes.

If :bcrypt is used, then instead of calling BasicAuth.make_passwd (which uses crypt), WEBrick::HTTPAuth::Htpasswd#set_passwd will set the bcrypt password directly. It isn't possible to change the make_passwd API to accept the password hash format, as that would break configurations who use Htpasswd#auth_type= to set a custom auth_type.

This modifies WEBrick::HTTPAuth::BasicAuth to handle checking both crypt and bcrypt hashes.

There are commented out requires for 'string/crypt', to handle when String#crypt is deprecated and the undeprecated version is moved to a gem.

There is also a commented out warning for the case when the password_hash keyword is not specified and 'string/crypt' cannot be required. I think the warning makes sense to nudge users to using bcrypt.

I've updated the tests to test nil, :crypt, and :bcrypt values for the password_hash keyword, skipping the bcrypt tests if the bcrypt library cannot be required.

[ruby-core:88111] [Feature #14940]

From: Jeremy Evans code@jeremyevans.net

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@64060 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 07/26/2018 03:21 AM - normalperson (Eric Wong)

- Status changed from Open to Closed

Applied in changeset trunk|r64060.

---

webrick: Support bcrypt password hashing

This adds a password_hash keyword argument to WEBrick::HTTPAuth::Htpasswd#initialize. If set to :bcrypt, it will create bcrypt hashes instead of crypt hashes, and will raise an exception if the .htpasswd file uses crypt hashes.

If :bcrypt is used, then instead of calling BasicAuth.make_passwd (which uses crypt), WEBrick::HTTPAuth::Htpasswd#set_passwd will set the bcrypt password directly. It isn't possible to change the make_passwd API to accept the password hash format, as that would break configurations who use Htpasswd#auth_type= to set a custom auth_type.

This modifies WEBrick::HTTPAuth::BasicAuth to handle checking both crypt and bcrypt hashes.

There are commented out requires for 'string/crypt', to handle when String#crypt is deprecated and the undeprecated version is moved to a gem.

There is also a commented out warning for the case when the password_hash keyword is not specified and 'string/crypt' cannot be required. I think the warning makes sense to nudge users to using bcrypt.

I've updated the tests to test nil, :crypt, and :bcrypt values for the password_hash keyword, skipping the bcrypt tests if the bcrypt library cannot be required.

[ruby-core:88111] [Feature #14940]

From: Jeremy Evans code@jeremyevans.net

#2 - 07/26/2018 03:32 AM - normalperson (Eric Wong)

Thanks, applied as r64060.

I needed to add RUBYLIB=/path/to/bcrypt/lib to my make command line to test bcrypt; but I suppose that's fine

#3 - 05/22/2019 05:03 AM - akr (Akira Tanaka)

- Related to Feature #14915: Deprecate String#crypt added

Files

0001-Support-bcrypt-password-hashing-in-webrick.patch	12.8 KB	07/25/2018	jeremyevans0 (Jeremy Evans)