

Ruby master - Bug #5274

[ruby-dev:44460] Class clone Class

09/05/2011 07:15 AM - mrkn (Kenta Murata)

Status: Closed	
Priority: Normal	
Assignee: matz (Yukihiro Matsumoto)	
Target version: 1.9.3	
ruby -v: ruby 1.9.3dev (2011-09-04 revision 33179)	Backport:

Description

[ruby-dev:44460]

```
segv
Ruby ruby 1.9.3dev (2011-09-04 revision 33179)
[i686-linux]

#(
StrClone = String.clone
Class.new(StrClone)
Marshal.dump(StrClone.new("a"))

segv StrClone.new("a")
Class.new(StrClone) StrClone
StrClone T_STRING
T_OBJECT StrClone.new T_OBJECT

StrClone
T_OBJECT
Marshal.dump
segv

class clone
StrClone
StrClone
make_metaclass(class.c)

#define ENSURE_EIGENCLASS(klass) \
(rb_ivar_get(METACLASS_OF(klass), id_attached) == (klass) ? \
METACLASS_OF(klass) : make_metaclass(klass))

static inline VALUE
make_metaclass(VALUE klass)
{
....

super = RCLASS_SUPER(klass);
while (RB_TYPE_P(super, T_ICLASS)) super = RCLASS_SUPER(super);
RCLASS_SUPER(metaclass) = super ? ENSURE_EIGENCLASS(super) : rb_cClass;

....

return metaclass;
}
```

```

    ENSURE_EIGENCLASS klass StrClone
    rb_ivar_get(METACLASS_OF(StrClone), id_attached) == (StrClone)
    make_metaclass(StrClone)
    make_metaclass(StrClone) StrClone

    "attached"
    StrClone
    "attached" rb_singleton_class_clone(class.c)
    "attached" StrClone StrClone

VALUE
rb_singleton_class_clone(VALUE obj)
{
    VALUE klass = RBASIC(obj)->klass;
    ...
    VALUE clone = class_alloc((RBASIC(klass)->flags & ~(FL_MARK)), 0);
    if (BUILTIN_TYPE(obj) == T_CLASS) {
        RBASIC(clone)->klass = (VALUE)clone; /* <= (1) */
    }
    else {
        RBASIC(clone)->klass = rb_singleton_class_clone(klass);
    }
    rb_singleton_class_attached(RBASIC(clone)->klass, (VALUE)clone);
    /* (1) RBASIC(clone)->klass = clone */
    /* clone "_attached_" clone */
    ...
}

rb_singleton_class_clone "attached"
"attached"
class.c

"attached"
test-all


```

Index: object.c

```

--- object.c (revision 33182)
+++ object.c (working copy)
@@ -272,12 +272,17 @@
rb_obj_clone(VALUE obj)
{
    VALUE clone;

    • VALUE singleton;

    if (rb_special_const_p(obj)) {
        rb_raise(rb_eTypeError, "can't clone %s", rb_obj_classname(obj));
    }
    clone = rb_obj_alloc(rb_obj_class(obj));

```


- object.c (rb_obj_clone): singleton class should be attached singleton object to. a patch by Satoshi Shiba at [ruby-dev:44460]. [Bug #5274]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@33292 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 33292 - 09/18/2011 10:54 PM - nobu (Nobuyoshi Nakada)

- object.c (rb_obj_clone): singleton class should be attached singleton object to. a patch by Satoshi Shiba at [ruby-dev:44460]. [Bug #5274]

Revision 33292 - 09/18/2011 10:54 PM - nobu (Nobuyoshi Nakada)

- object.c (rb_obj_clone): singleton class should be attached singleton object to. a patch by Satoshi Shiba at [ruby-dev:44460]. [Bug #5274]

Revision 33292 - 09/18/2011 10:54 PM - nobu (Nobuyoshi Nakada)

- object.c (rb_obj_clone): singleton class should be attached singleton object to. a patch by Satoshi Shiba at [ruby-dev:44460]. [Bug #5274]

Revision 33292 - 09/18/2011 10:54 PM - nobu (Nobuyoshi Nakada)

- object.c (rb_obj_clone): singleton class should be attached singleton object to. a patch by Satoshi Shiba at [ruby-dev:44460]. [Bug #5274]

Revision 33292 - 09/18/2011 10:54 PM - nobu (Nobuyoshi Nakada)

- object.c (rb_obj_clone): singleton class should be attached singleton object to. a patch by Satoshi Shiba at [ruby-dev:44460]. [Bug #5274]

Revision 33292 - 09/18/2011 10:54 PM - nobu (Nobuyoshi Nakada)

- object.c (rb_obj_clone): singleton class should be attached singleton object to. a patch by Satoshi Shiba at [ruby-dev:44460]. [Bug #5274]

History

#1 - 09/19/2011 07:54 AM - nobu (Nobuyoshi Nakada)

- Status changed from *Assigned* to *Closed*

- % Done changed from 0 to 100

This issue was solved with changeset r33292.
Kenta, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- object.c (rb_obj_clone): singleton class should be attached singleton object to. a patch by Satoshi Shiba at [ruby-dev:44460]. [Bug [#5274](#)]