RhodeCode CE/EE - Support #5544

Use of authentication token with LDAP account results in account lockout when max bad password attempts are configured in LDAP

26.02.2019 23:03 - John Henning

Status:	Resolved	**Start date:**	26.02.2019
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour
Sorting:		**Affected Version:**	v4.12
Commit Number:			

Description

(Using the Community Edition)

We would like to use the authentication tokens for accounts used by automated systems. In our organization these "service" accounts are required to be managed in Active Directory/LDAP. Normally this is fine since Rhodecode works great with LDAP accounts. However, mixing an LDAP account with authentication token usage is an issue because of an LDAP configuration requirement for account lockout after a number of bad password attempts, and also general security monitoring of failed logins.

When using the authentication token to authenticate to Rhodecode, Rhodecode first attempts to authenticate the LDAP user against LDAP using the token as the password. This obviously fails thus incrementing the bad password counter (eventually locking the account) and also logging a failed login attempt in the monitoring of the LDAP system.

I have focused primarily on the service accounts in this filing, but this could also affect users that opt to use the token on shared systems where they would prefer to not record their LDAP password.

While the account is still technically usable in Rhodecode, this behavior creates a situation where the security monitoring of the accounts is muddied by the false failures. Is there a way to change the order in which Rhodecode attempts authentication to have it first verify against the authentication token rather than LDAP?

Related log output:

```
[26/Feb/2019:16:37:04 -0500] GNCRN <63245>  127.0.0.1       rqt:0.471118 200 42 "GET:/repogroup/re
po cmd=batch" usr:serviceaccount "-" "mercurial/proto-1.0"
2019-02-26 16:37:04.111 [54043] INFO  [rhodecode.authentication.base] Authenticating user `service
account` using egg:rhodecode-enterprise-ce#ldap plugin
2019-02-26 16:37:04.375 [54043] ERROR [rhodecode.authentication.plugins.auth_ldap] LDAP related ex
ception
Traceback (most recent call last):
  File "/opt/rhodecode/store/p9vr3b65srfrkr4gbag23mpcdkk0xy6w-python2.7-rhodecode-enterprise-ce-4.
12.4/lib/python2.7/site-packages/rhodecode/authentication/plugins/auth_ldap.py", line 463, in auth
    (user_dn, ldap_attrs) = aldap.authenticate_ldap(username, password)
  File "/opt/rhodecode/store/p9vr3b65srfrkr4gbag23mpcdkk0xy6w-python2.7-rhodecode-enterprise-ce-4.
12.4/lib/python2.7/site-packages/rhodecode/authentication/plugins/auth_ldap.py", line 338, in auth
enticate_ldap
    'with given password'.format(username))
LdapPasswordError: Failed to authenticate user `serviceaccount`with given password
2019-02-26 16:37:04.385 [54043] INFO  [rhodecode.authentication.base] Authenticating user `service
account` using egg:rhodecode-enterprise-ce#token plugin
2019-02-26 16:37:04.402 [54043] INFO  [rhodecode.authentication.plugins.auth_token] user `servicea
ccount` successfully authenticated via authtoken
2019-02-26 16:37:04.402 [54043] INFO  [rhodecode.lib.middleware.simplevcs] MAIN-AUTH successful fo
r user `serviceaccount` from authtoken plugin
2019-02-26 16:37:04.413 [54043] INFO  [rhodecode.lib.middleware.simplevcs] Access for IP:xxx.xxx.x
xx.xxx allowed
2019-02-26 16:37:04.491 [54043] INFO  [rhodecode.lib.middleware.simplevcs] pull action on hg repo
"repogroup/repo" by "serviceaccount" from xxx.xxx.xxx.xxx mercurial/proto-1.0
2019-02-26 16:37:04.500 [54043] INFO  [rhodecode.lib.middleware.simplevcs] Using HTTP implementati
on of scm app.
```

```
2019-02-26 16:37:04.546 [54043] INFO  [rhodecode.lib.middleware.request_wrapper] IP: xxx.xxx.xxx.xxx Request to /repogroup/repo time: 0.481s [mercurial/proto-1.0]
```

History

#1 - 26.02.2019 23:14 - Marcin Kuzminski [staff]

Hi John,

Yes indeed there's a simple way to configure the order. In the authentication plugin administration screen you'll see a list of enabled plugins in a text field comma separated, simply put the token one before LDAP and RhodeCode would try token first followed by LDAP. That should fix the problem you're having.

Best,

#2 - 26.02.2019 23:24 - John Henning

Marcin Kuzminski [staff] wrote:

> Hi John,
>
> Yes indeed there's a simple way to configure the order. In the authentication plugin administration screen you'll see a list of enabled plugins in a text field comma separated, simply put the token one before LDAP and RhodeCode would try token first followed by LDAP. That should fix the problem you're having.
>
> Best,

Cannot believe I missed that.

Thank you!

#3 - 26.02.2019 23:27 - John Henning

Does this require a restart of Rhodecode to take effect or is it immediate?

#4 - 27.02.2019 10:09 - Marcin Kuzminski [staff]

- Status changed from New to Resolved

I belive there's some caches, best to restart that should invalidate cache for the settings.