# FreeNAS - Feature #1403

## Active Directory admin password is stored in the config database

03/15/2012 04:28 PM - Manolis -

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Estimated time:** | 0.00 hour |
| **Priority:** | Nice to have | | |
| **Assignee:** | John Hixson | | |
| **Category:** | Middleware | | |
| **Target version:** | 9.2.1-RELEASE | | |
| **Severity:** | New | **Needs Merging:** | Yes |
| **Reason for Closing:** | | **Needs Automation:** | No |
| **Reason for Blocked:** | | **Support Suite Ticket:** | n/a |
| **Needs QA:** | Yes | **Hardware Configuration:** | |
| **Needs Doc:** | Yes | | |

**Description**

After joining an Active Directory (AD) domain, the admin password entered in the web gui form is stored in the config database (/data/freenas-v1.db) in plaintext.

```
[root@zbox0] ~# /usr/local/bin/sqlite3 /data/freenas-v1.db
SQLite version 3.7.7.1 2011-06-28 17:39:05
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> select ad_domainname, ad_adminpw from services_activedirectory;
domain.com|DOMAIN_ADMIN_PASSWORD
sqlite>
```

This could lead to a major security incident: An attacker successfully compromising the local root account of [[FreeNAS]] will also gain admin access to the AD, using the stored password.

Additionally, in deployments where AD is centrally and [[FreeNAS]] locally administered, it means that in order to enable AD authentication on [[FreeNAS]] the AD administrator will have to yield the AD admin password to all [[FreeNAS]] administrators. This would be simply unacceptable in most cases.

This problem can be fixed by serializing and storing the host credential files (secrets.tdb et al) in the database. This way the AD administrator password won't have to be stored.

Note: The serialization (base64 encoding) and storing of files in the database has already been implemented by ssh for making /etc/ssh/ssh_host_* files pesistent. It can be found in /etc/rc.d/sshd.

**Related issues:**

| | | |
|---|---|---|
| Has duplicate FreeNAS - Bug #3325: AD Domain Admin password is stored in clea... | **Closed: Duplicate** | 10/18/2013 |

### Associated revisions

**Revision 46ae467c - 12/30/2013 01:02 AM - John Hixson**

Rework Active Directory code to make use of kerberos keytabs

- Renamed ad_adminname and ad_adminpw to more generic ad_bindname and ad_bindpw
- Created necessary migration to do the rename and preserve the contents
of the old fields
- Modified all code that references those names accordingly
- Added ad_keytab field and ad_use_keytab to specify using a keytab
- Modified ix-kinit to use kerberos keytab if present
- ad_bindname and ad_bindpw are overloaded now, if not using a keytab, they
work like ad_adminname and ad_adminpw did. Administrator credentials
can be used. If using a keytab, a less privileged user account should
be used that has sufficient privilege to perform LDAP queries. The

keytab used should have privileges to grant tickets for cifs and ldap
(host/*) should work. A keytab can be created on windows like so:

```
ktpass.exe -out hostname.keytab -princ host/hostname@DOMAINNAME -ptype
      KRB5_NT_PRINCIPAL -mapuser DOMAIN\username -pass userpass
```

```
setspn -A host/hostname@DOMAINNAME DOMAIN\username
```

```
If done correctly, once the keytab is generated, it can be uploaded to
  FreeNAS through the GUI and then click on the option to use a keytab
  and Active Directory joins will be passwordless ;-)
```

Ticket: #1403

### History

**#1 - 10/18/2013 07:32 PM - William Grzybowski**

*- Target version changed from 8.2.0-RELEASE to 19*

*- Seen in set to 9.1.1-RELEASE*

**#2 - 11/11/2013 05:50 PM - Jordan Hubbard**

*- Target version changed from 19 to 59*

**#3 - 12/14/2013 03:04 AM - Jordan Hubbard**

*- Assignee set to John Hixson*

*- Target version changed from 59 to 9.2.0-RELEASE*

John, is this still true?  We should try and whack it for 9.2.0-RELEASE if so!

**#4 - 12/15/2013 01:15 AM - John Hixson**

*- Status changed from Unscreened to Screened*

**#5 - 12/16/2013 07:24 PM - Jordan Hubbard**

*- Target version changed from 9.2.0-RELEASE to 62*

Looks like we can't get this fix for 9.2.0 - it's a complex issue.  We agree that it's a problem (security concern) but the fix is "hard".

**#6 - 12/16/2013 09:59 PM - Manolis -**

Jordan Hubbard wrote:

Looks like we can't get this fix for 9.2.0 - it's a complex issue.  We agree that it's a problem (security concern) but the fix is "hard".

Hi Jordan,
Could you elaborate?
To my best knowledge all you have to do is serialize a bunch of .tdb files and restore them on startup. Wouldn't that be enough? Are there any hidden side-effects to this?

#### #7 - 12/24/2013 09:50 PM - John Hixson

*- Tracker changed from Bug to Feature*

#### #8 - 12/24/2013 10:23 PM - Manolis -

"Tracker changed from Bug to Feature"

Is this some kind of joke? Like: "It's not a bug - it's a feature. It allows you to recover your AD password in case you ever lose the postit note you had written it on."

This makes FreeNAS a **GAPING HOLE** for the security of the network it is deployed on. It's the same as writting down the AD password in a plaintext file. Could you please take the issue more seriously? This bug is here for two years and the only action taken was to downplay it to a "Feature". Don't take any action if you don't feel like it, but don't downplay the issue and add a warning in the documentation to let the users know.

On the side of this, have a very merry Christmas!

#### #9 - 12/24/2013 10:31 PM - Josh Paetzel

The classification is arbitrary between a bug and feature.

We agree with your points wholeheartedly and regret it didn't make it for 9.2.0, however fixing this is a high priority.

#### #10 - 12/30/2013 09:16 AM - John Hixson

*- Status changed from Screened to Resolved*

*- Priority changed from Expected to Nice to have*

The ability to join Active Directory without saving the Administrator password in the database now exists via 46ae467cbff9409f55dd4167b87a7808d196d9ef. Keep in mind that you can still use Administrator username/password if you choose. If not, you can use a kerberos keytab and a less privileged account for performing the LDAP queries that are necessary (but the password still remains in the database). I consider this acceptable and am marking this ticket as resolved.

#### #11 - 01/20/2014 07:36 AM - Jordan Hubbard

*- Status changed from Resolved to Closed*

#### #12 - 05/23/2015 11:43 PM - Jordan Hubbard

- Target version changed from 62 to 9.2.1-RELEASE