From: Spitzer, Andras ( )
Sent: Saturday, July 27, 2013 7:45 PM
To:)
Cc: ( ); ( ); ( ); ( ) ( ); ( ); ( )
Subject: NSSLTOF & SAPM support
Attachments: NSSLTOF_PAM_scripts.tar

Bob,

The problem we identified on **non-Likewise servers with NSSLTOF enabled** and which breaks SAPM :

1. If you try to change the password for a local user, you get the following message (this is not specific to NSSLTOF, Solaris acts the same with any NSS module which is not part of Core Solaris):

```
root@isslabsol03 #passwd nobody
passwd: Unsupported nsswitch entry for "passwd:". Use "-r repository ".
Unexpected failure. Password file/table unchanged.
```

Even though we can use the 'passwd –r files <username>' command in this case, **SAPM doesn't know that** so it won't update local passwords.

Proposed **solution** (created since yesterday) is a PAM addon for NSSLTOF :

2. pkgadd –d http://lonperf01.corporate. p/ISSnssl2fPAM.pkg , this will **install NSSLTOF PAM module**
3. **execute the PAM enabler script** attached to this e-mail, **enable_nssltof_pam.sh,** this will add one line into /etc/pam.conf

Try **1. again, you should see passwd** works again.

Details :

I investigated the root cause of the problem, and **Likewise enabled servers are not affected**. The problem comes from the fact that a PAM module (pam_passwd_auth.so.1) which is used only at the 'passwd' service will start scanning the nsswitch.conf for backend sources, and when it encounters an unknown database (which is basically any 3rd party module like lsass or issc) it gives the error message we saw at 1. There is one exception though and that it what Likewise use to avoid this. If the default PAM repository is set to 'files' before PAM gets to this module, it will not scan the nsswitch.conf but it will use the default one.

So **Likewise servers are not affected because** they have **this line** in /etc/pam.conf :

```
passwd auth requisite pam_lsass.so set_default_repository
```

So I created a simple PAM module for issc as well, which only sets the default PAM repo to files. The package you install at step **2.** will **install the PAM module**, and the script at **3.** will **add this line** into /etc/pam.conf :

```
passwd  auth requisite          pam_issc.so.1
```

right before the pam_passwd_auth.so.1 line. **This way pam_issc.so.1 sets the default PAM repository, and pam_passwd_auth.so.1 doesn't have to scan nsswitch.conf**.

I could have add the PAM enabler/disabler scripts as postinstall/postremove scripts, but because of our sparse zones I decided to package them separately, making it more flexible.

If you tested the solution and it works, I would like to recommend :

1. **install ISSnssl2fPAM.pkg on all the existing NSSLTOF enabled hosts**, it won't harm anything, no conflicting files, no change in any configuration
2. **run the NSSLTOF PAM enabler script** on all the NSSLTOF enabled hosts, including the Likewise enabled ones

Rollback plan :

1. just **restore the original pam.conf** which is saved as /etc/pam. conf_PRENSSLTOFPAM (or use my attached PAM disabler script, called disable_nssltof_pam.sh)
2. remove the NSSLTOF PAM package with 'pkgrm ISSnssl2fPAM' (this is optional as the PAM files won't do anything, this is only cleanup)

Even though the Likewise enabled servers are not affected hence they do not benefit from this, s ll I would install and enable there too for consistency, as it cause no harm. The 1. PAM package contains no conflic ng files 2. the PAM enabler adds a single line only for the 'passwd' service, and it only sets the default PAM repo to 'files' if it's not already set. This on the Likewise servers will do nothing, Likewise already sets the default PAM repo, so the module will just return.

This should remediate all of our SAPM & NSSLTOF compa bility problems on the exis ng installa ons.

About the **future NSSLTOF installa ons**.

Today we ended up having two packages, the original core NSSLTOF package (ISSnssl2f) and the PAM addon package (ISSnssl2fPAM) released today. The reason why I created the PAM module package because this way we don't have to upgrade the exis ng NSSLTOF packages, we only have to add the new PAM module package.

S ll, because I want to keep the package simple, I updated the original NSSLTOF package (all the earlier versions are 0.5, this latest is 0.6) at http://lonperf01.corporate.[redacted]p/ISSnssl2f.pkg so the new package installs the PAM module as well, so for new installs we don't need the PAM addon package. It installs the PAM enabler/disabler scripts under misc/script too, but it does not enable it during the install so pam.conf remains unchanged. So Bob, I would like to ask you to update the NSSLTOF package within Opsware with the latest package from http://lonperf01.corporate.[redacted]p/ISSnssl2f.pkg, and we should extend the post-install scripts in Opsware so it updates /etc/pam.conf as my PAM enabler script does.

sendai