FreeNAS - Bug #6951

ix-activedirectory is deleting computer object on service stop

12/04/2014 10:48 AM - Duncan Fraser

Status:	Resolved		
Priority:	Important		
Assignee:	John Hixson		
Category:	OS		
Target version:	N/A		
Seen in:	9.2.1.9-RELEASE	**Needs Merging:**	Yes
Severity:	New	**Needs Automation:**	No
Reason for Closing:		**Support Suite Ticket:**	n/a
Reason for Blocked:		**Hardware Configuration:**	
Needs QA:	Yes	**ChangeLog Required:**	No
Needs Doc:	Yes		

Description

ix-activedirectory is deleting computer object on service stop. When turning off directory services for troubleshooting/reconfiguration via the WebGUI, or stopping ix-activedirectory via shell, the computer object for FreeNAS is being deleted.

This is contrary to typical AD behavior, and complicates the use of FreeNAS in large AD environments. Standard behavior should be the disable the computer object, not delete. Otherwise, every time the service is bounced, all security permissions and OU placement is lost. This circumvents our security procedures, as we give FreeNAS a service account that has permissions explicitly granted for the FreeNAS computer objects only. Once the object is deleted, FreeNAS is not able to rebind.

Seen in 9.2.1.9 and 9.3 BETA.

Output from ix-activedirectory:
[root@***-***-store01] /mnt/vol1# service ix-activedirectory stop
Deleted account for '***-***-STORE01' in realm '**.**.*****.***'
[root@***-***-store01] /mnt/vol1# service ix-activedirectory start
Failed to join domain: failed to set machine spn: Constraint violation

Associated revisions

Revision 14f60a64 - 07/13/2015 10:16 PM - John Hixson

Methods for enabling and disabling of machine accounts in AD

Ticket: #6951

Revision c9a095d1 - 07/14/2015 09:37 PM - John Hixson

Don't blow away computer object when disabling AD

Ticket: #6951
Merge-FN93: yes
Merge-TN93: yes

Revision d416f572 - 07/15/2015 05:09 PM - John Hixson

Methods for enabling and disabling of machine accounts in AD

Ticket: #6951

Revision ba99601d - 07/15/2015 05:09 PM - John Hixson

Don't blow away computer object when disabling AD

Ticket: #6951
Merge-FN93: yes
Merge-TN93: yes
(cherry picked from commit c9a095d17ebdf80e516775e11061745b4ef36049)

Revision 9828cb53 - 07/15/2015 05:10 PM - John Hixson

Methods for enabling and disabling of machine accounts in AD

Ticket: #6951
(cherry picked from commit 14f60a64d9a20e3123dd8833cb1e380c31299fd6)

Revision 61162e29 - 07/15/2015 05:10 PM - John Hixson

Don't blow away computer object when disabling AD

Ticket: #6951
Merge-FN93: yes
Merge-TN93: yes
(cherry picked from commit c9a095d17ebdf80e516775e11061745b4ef36049)

History

#1 - 12/04/2014 12:39 PM - Jordan Hubbard

- Category set to 36

- Status changed from Unscreened to Screened

- Assignee set to John Hixson

- Target version set to 49

BRB: This is going to be complicated to fix since that is not how our AD system is currently designed. Setting milestone accordingly, since we don't know when/if this will be fixed.

#2 - 12/06/2014 07:22 PM - Duncan Fraser

Thinking of possible work-arounds, I set the computer object to Prevent Accidental Deletion in AD. Now, ix-activdirectory explicitly states "Disabling account for 'test-freenas01' in realm '**.**.*****.***' on service stop and restart.

Looks like ix-activedirectory has some awareness of disabled accounts.

#3 - 06/30/2015 02:00 AM - John Hixson

- Target version changed from 49 to Unspecified

I think now is a good time to work on this.

#4 - 07/02/2015 08:59 AM - John Hixson

I pulled this ticket into 9.3 as a SU candidate because I've now seen a few cases where this matters. I am hoping to start working on this next week.

#5 - 07/06/2015 11:31 AM - John Hixson

Hopefully this week ;-) We will see

#6 - 07/06/2015 11:37 AM - John Hixson

- Priority changed from Nice to have to Important

#7 - 07/07/2015 09:52 PM - John Hixson

This is next on my list. I have to finish up what I'm working on then I'll be tackling this. Coming soon!

#8 - 07/09/2015 12:11 AM - John Hixson

If I don't start this by the end of this week, I will definitely be starting beginning of next week.

#9 - 07/10/2015 12:38 AM - John Hixson

Looks like next week for this

#10 - 07/13/2015 03:36 PM - John Hixson

- Status changed from Screened to Investigation

Looking into this now ;-)

#11 - 07/13/2015 11:02 PM - John Hixson

I've written some methods for enabling and disabling the machine account. More to come.

#12 - 07/14/2015 08:20 PM - John Hixson

- % Done changed from 0 to 10

I've been working on not leaving the domain, and not joining it if it's already joined. It's taking more consideration than I originally thought ;-) So, hopefully I'll have this done this week. Honestly I think the entire AD architecture probably needs a little bit of an overhaul.

#13 - 07/14/2015 11:07 PM - John Hixson

I've got this at a point where it is working. It's not exactly elegant but it does what you want ;-) Just waiting to merge this to the correct places then will mark it ready for release.

#14 - 07/15/2015 05:12 PM - John Hixson

- Status changed from Investigation to Ready For Release

merged and ready to go

#15 - 08/25/2015 10:53 AM - Jordan Hubbard

- Status changed from Ready For Release to Resolved

#16 - 08/26/2016 01:53 PM - Kris Moore

- Target version changed from Unspecified to N/A