FreeNAS - Bug #28209

Add unix_primary_group and unix_nss_info to idmap_ad configuration to address how Samba now handles groups

02/05/2018 07:54 PM - Charles West

Status:	Done		
Priority:	Important		
Assignee:	John Hixson		
Category:	OS		
Target version:	11.2-BETA2		
Seen in:	11.1-U1	**Needs Merging:**	No
Severity:	Medium	**Needs Automation:**	No
Reason for Closing:		**Support Suite Ticket:**	n/a
Reason for Blocked:		**Hardware Configuration:**	
Needs QA:	No	**ChangeLog Required:**	No
Needs Doc:	No		

Description

Samba authentication using the 'ad' backend and gid user/group attributes worked in 9.10.2, but is broken in 11.1-U1 for users relying on the gidNumber LDAP attribute. It appears Samba was upgraded from 4.5.5 to 4.7.0 between 9.10.2 and 11.1-U1. The Samba wiki identifies a difference in the way that it handles groups starting in 4.6.0 (see https://wiki.samba.org/index.php/Idmap_config_ad#The_RFC2307_and_template_Mode_Options).

With Samba's new unix_primary_group default setting, the primaryGroupID attribute is used to determine the gid for users, and not the gidNumber. The primaryGroupID is set to the last part of the AD group's ObjectSid. The ObjectSid is read-only and cannot be modified which results in AD users not being recognized by Samba when their primary group's ObectSid falls outside the idmap config range.

Using the Web UI-generated /usr/local/etc/smb4.conf, my AD groups are presented via getent group because the gidNumber I assigned them falls within the idmap config range. My AD users are not presented via getent passwd since their primary group's ObjectSid falls outside the idmap config range. After adding idmap config MYDOMAIN: unix_primary_group = yes line to /usr/local/etc/smb4.conf and running /usr/local/etc/rc.d/samba_server restart, I can now see the AD users and assign permissions to them within FreeNAS.

It seems that this is largely a Samba issue, since with default settings Samba would seemingly break their own multi-domain integration with non-overlapping ranges due to arbitrarily assigned ObjectSid values. However, it would be extremely helpful if FreeNAS could guard against this issue by inserting MYDOMAIN: unix_primary_group = no into smb4.conf and providing a deterministic way to import users and groups from AD into FreeNAS.

Is it possible to get MYDOMAIN: unix_primary_group = no added to smb4.conf to accommodate the 'ad' backend? I'm willing to test other workarounds. Thanks!

PS: Please let me know if any of my assertions are incorrect. For my setup, I have multiple users and groups all configured with uidNumber, gidNumber, loginShell, and unixHomeDirectory attributes defined, added to the Global Catalog, etc. I'm using a "stock" Windows Server 2016 domain controller. Users and groups are defined, but no Group Policy, OUs, or anything fancy(TM).

Related issues:

Copied to FreeNAS - Bug #40708: Add unix_primary_group and unix_nss_info to i...	**Done**

Associated revisions

Revision 1c151e30 - 06/14/2018 02:50 PM - John Hixson

Add unix_primary_group and unix_nss_info to idmap_ad configuration

Ticket: #28209

Revision 1dfc20db - 08/03/2018 11:54 AM - John Hixson

Add unix_primary_group and unix_nss_info to idmap_ad configuration

Ticket: #28209
(cherry picked from commit 1c151e301cf88552be5b833cb3767e52942c9d88)

(11.1-stable)
Ticket: #40708

History

#1 - 02/06/2018 04:13 AM - Dru Lavigne

- Category changed from Middleware to OS

- Assignee changed from Release Council to John Hixson

- Target version set to 11.2-RC2

#2 - 03/28/2018 11:21 PM - John Hixson

- Assignee changed from John Hixson to Timur Bakeyev

#3 - 04/20/2018 07:40 PM - Timur Bakeyev

- Severity set to Medium

#4 - 06/13/2018 08:55 AM - John Hixson

- Assignee changed from Timur Bakeyev to John Hixson

#5 - 06/13/2018 02:14 PM - John Hixson

This is a simple fix. Coming soon.

#6 - 06/14/2018 02:52 PM - John Hixson

1c151e301cf88552be5b833cb3767e52942c9d88
PR: https://github.com/freenas/freenas/pull/1370

#7 - 06/14/2018 02:53 PM - John Hixson

- Status changed from Not Started to Ready for Testing

#8 - 06/14/2018 03:26 PM - Dru Lavigne

- Subject changed from Samba 'ad' idmap group handling prevents user import to Add unix_primary_group and unix_nss_info to idmap_ad configuration to address how Samba now handles groups

- Status changed from Ready for Testing to In Progress

#9 - 06/28/2018 07:10 AM - Dru Lavigne

- Target version changed from 11.2-RC2 to 11.2-BETA2

#10 - 06/28/2018 12:10 PM - John Hixson

- Status changed from In Progress to Ready for Testing

#11 - 06/29/2018 06:13 AM - Dru Lavigne

- Status changed from Ready for Testing to In Progress

#12 - 07/10/2018 12:03 PM - John Hixson

- Status changed from In Progress to Ready for Testing

#13 - 07/10/2018 07:19 PM - Dru Lavigne

- Needs Doc changed from Yes to No

- Needs Merging changed from Yes to No

#15 - 07/20/2018 07:18 AM - John Hixson

Charles, This code is currently in 11.2BETA (or the nightlies). Can you verify this is working for you?

#16 - 07/25/2018 01:53 PM - Bonnie Follweiler

- Status changed from Ready for Testing to Passed Testing

- Needs QA changed from Yes to No

#18 - 07/26/2018 06:22 AM - Dru Lavigne

- Status changed from Passed Testing to Done

#19 - 08/03/2018 11:54 AM - John Hixson

- Copied to Bug #40708: Add unix_primary_group and unix_nss_info to idmap_ad configuration to address how Samba now handles groups added