

FreeNAS - Feature #27584

Get DC/GC SRV records from the default site if DNS is broken in local site

01/03/2018 06:06 AM - Emanuel Klein

Status: Done	Estimated time: 0.00 hour
Priority: No priority	
Assignee: Andrew Walker	
Category: Services	
Target version: 11.3-ALPHA1	
Severity: Low Medium	Needs Merging: No
Reason for Closing:	Needs Automation: No
Reason for Blocked:	Support Suite Ticket: n/a
Needs QA: No	Hardware Configuration:
Needs Doc: No	

Description

Assuming two Active Directory Sites. Domain Controller in Site A. FreeNAS in Site B.
Assuming a working DNS infrastructure with properly set resolver/forwarder on FreeNAS.

Current behaviour

Upon joining a domain using basic settings

- 1) The script properly resolves the site in which FreeNAS currently resides. -> SiteB
- 2) The script tries to contact a DC in its current site. -> no DC available
<service>.<SiteB>._sites.dc._msdcs.<domain>
- 3) The join process fails

Upon joining a domain using advanced settings,

- 1) "hardcoding" SiteA - where an active DC resides.
- 2) The script properly resolves services in the hardcoded SiteA.
<service>.<SiteA>._sites.dc._msdcs.<domain>
- 3) The join process succeeds

Drawback of this variant is lost resiliency when SiteA is not reachable, but potential other DCs available in potential other Sites.

Expected behaviour -> Standard Windows Client behaviour

- 1) The script fails to contact a DC in its local site
<service>.<SiteB>._sites.dc._msdcs.<domain>
- 2) The script performs a fallback lookup to find non site-specific services.
<service>.dc._msdcs.<domain>

This will also fix the drawback mentioned when "hardcoding" the site.

History

#1 - 01/03/2018 08:33 AM - Dru Lavigne

- Assignee changed from Release Council to John Hixson

- Target version set to 11.3

- Seen in changed from TrueNAS 11.1-U1 to 11.1

#2 - 01/12/2018 11:03 AM - John Hixson

- Status changed from Unscreened to Screened

#3 - 01/29/2018 07:32 AM - Kris Moore

- Status changed from Screened to Not Started

#4 - 03/28/2018 11:22 PM - John Hixson

- Assignee changed from John Hixson to Timur Bakeyev

#5 - 04/20/2018 07:46 PM - Timur Bakeyev

- Severity set to Low Medium

#6 - 04/27/2018 11:37 AM - Ben Gadd

- Target version changed from 11.3 to Backlog

#7 - 08/09/2018 01:58 PM - Timur Bakeyev

- Tracker changed from Bug to Feature
- Category changed from OS to Services
- Status changed from Not Started to Screened
- Seen in deleted (11.1)
- ChangeLog Required deleted (No)

#8 - 08/09/2018 02:02 PM - Timur Bakeyev

- Target version changed from Backlog to 11.3
- Needs Doc changed from Yes to No
- Needs Merging changed from Yes to No

That sounds as a reasonable idea, but we need to make sure that there are no drawbacks of such a change.

#9 - 08/23/2018 10:55 AM - Dru Lavigne

- Assignee changed from Timur Bakeyev to John Hixson

#10 - 10/15/2018 10:14 AM - Dru Lavigne

- Assignee changed from John Hixson to William Grzybowski

#11 - 10/17/2018 09:52 AM - William Grzybowski

- Status changed from Screened to Unscreened
- Assignee changed from William Grzybowski to Andrew Walker
- Target version changed from 11.3 to Backlog

#12 - 10/19/2018 09:52 PM - Andrew Walker

The situation is now different in 11.1-U6. The proper procedure in the circumstances laid out above is to hardcode Site A.

This site will be used for operations where we rebuild the directory service cache, and we will try to use it to regenerate the smb4.conf file; however, if the site is unavailable we now leave the smb4.conf file configured and samba running. This means that services should not be interrupted while the winbind connection manager transitions to the next available DC.

The key manual configuration step (apart from hardcoding the site) is to also add multiple servers (space delimited list) in the advanced settings for your kerberos realm. The list should be in order of preference.

Eventually, the issue in the ticket will need to be resolved by reworking how some of our ancillary directory service code works, but the reported issue can now be worked around.

#13 - 10/19/2018 10:09 PM - Andrew Walker

- Status changed from *Unscreened* to *Screened*

#17 - 12/05/2018 10:51 AM - Bug Clerk

- Status changed from *Screened* to *In Progress*

#18 - 12/05/2018 12:15 PM - Bug Clerk

- Status changed from *In Progress* to *Ready for Testing*

PR: <https://github.com/freenas/freenas/pull/2191>

#19 - 12/05/2018 12:15 PM - Bug Clerk

- Target version changed from *Backlog* to *11.3*

#20 - 12/09/2018 01:06 PM - Dru Lavigne

- Subject changed from *AD join fails with no Domain Controller in local site* to *Get DC/GC SRV records from the default site if DNS is broken in local site*

#21 - 01/21/2019 11:02 AM - Dru Lavigne

- Target version changed from *11.3* to *11.3-BETA1*

#24 - 03/28/2019 06:44 AM - Dru Lavigne

- Status changed from *Ready for Testing* to *Done*

- Needs QA changed from *Yes* to *No*

#26 - 04/02/2019 08:20 AM - Dru Lavigne

- Target version changed from *11.3-BETA1* to *11.3-ALPHA1*