How To Configure the Oracle ZFS Storage Appliance for Quest Authentication for Oracle Solaris

January 2014; v1.3
By Andrew Ness

This article describes how to configure Quest Authentication Services in the Oracle ZFS Storage Appliance to integrate Oracle Solaris 10 or Oracle Solaris 11 environments with Active Directory.

Quest Authentication Services (QAS) by Quest Software provide a cross-platform bridge between Windows-based Active Directory and authentication functions for other platforms, including UNIX (Oracle Solaris 10 and Oracle Solaris 11) and Linux.

When installed and configured, QAS allows nominated Active Directory users and groups to be represented on Oracle Solaris systems, providing a consistent Active Directory user or group to a Solaris User ID (UID) or group ID (GID). Oracle Solaris hosts can also verify passwords for the Active Directory.

Because Quest Authentication Services provide a single point of administration for UNIX and Windows users through Active Directory, permissions can be consistent for both platforms that share storage from an Oracle ZFS Storage Appliance.

Contents

Overview
Installing the Quest Authentication Services Agents on Oracle Solaris
Configuring the Oracle ZFS Storage Appliance for Active Directory and QAS
Verifying Correct Operation
Conclusion
References

Overview

When Active Directory (AD) is used to provide the directory services for users and groups, authentication must be performed on the AD framework. Due to the configuration of attributes under AD, the password field is not exported for external verification. Since only AD domain servers can provide authentication, Quest Authentication Services provide a necessary bridge to allow non-Windows platforms to authenticate against Active Directory.

QAS also provides a mapping between the Windows internal user and group identifiers and Oracle Solaris user and group IDs. This mapping is used by the Oracle ZFS Storage Appliance to ensure that consistent permissions and ownership of files is maintained among the differing platforms.

QAS is installed on the AD domain controller to provide the necessary changes to AD to be used by the agents installed on the Oracle Solaris clients. No additional software packages need to be installed on the Oracle ZFS Storage Appliance, but it may require some configuration changes in order to facilitate the mapping process.
Activating QAS for the Oracle ZFS Storage Appliance is a two-step process. First, you must configure the Oracle ZFS Storage Appliance to use AD services in the normal way. Next, you configure the mapping service to allow sharing of ownership and permission attributes to all the cooperating platforms.

The following figure shows the architecture of an example QAS deployment with the Oracle ZFS Storage Appliance.

![QAS deployment with the Oracle ZFS Storage Appliance](image)

**Figure 1. QAS deployment with the Oracle ZFS Storage Appliance**

**Installing the Quest Authentication Services Agents on Oracle Solaris**

This section provides a quick-start view of the procedure to install QAS agents on the Oracle Solaris host system. Consult the [Quest Authentication Services Installation Guide](www.quest.com/authentication-services/) for the full procedure and for further details.

1. Connect to a command-line interface (CLI) session on the Oracle Solaris host (using telnet, ssh, or the console).

2. Log in as root or a valid user and assume the root user role using the command `su` on the Oracle Solaris server.

3. Locate the installation media and license key files.

```
admin@quest:~$ su
Password:
root@quest# unzip -d QAS-Agents \ Quest_AuthenticationServicesSolarisAgents_403.zip
Archive: Quest_AuthenticationServicesSolarisAgents_403.zip
   creating: QAS-Agents/add-ons/
   creating: QAS-Agents/add-ons/smartcard/
   creating: QAS-Agents/add-ons/smartcard/solaris8-sparc/
   inflating: QAS-Agents/add-ons/smartcard/solaris8-sparc/vassc_SunOS_5.8_sparc-4.0.3.24.pkg
   creating: QAS-Agents/add-ons/siebel/
   creating: QAS-Agents/add-ons/siebel/solaris10-x64/
   inflating: QAS-Agents/add-ons/siebel/solaris10-x64/quest-mav_SunOS-ap20-3.6.7.i386.pkg
   inflating: QAS-Agents/add-ons/siebel/solaris10-x64/vassiebelad_SunOS_5.10_i386-4.0.3.24.pkg
   creating: QAS-Agents/add-ons/siebel/solaris8-x86/[…]
```
cd QAS-Agents
./install.sh

Quest Authentication Services Installation Script
Script Build Version: 4.0.3.24
Copyright 2011 Quest Software, Inc. ALL RIGHTS RESERVED.

Host Name: quest
Operating System: SunOS 11 (x86_64)

Checking for recommended patches...Done
Checking for available software... Done
Checking for installed software... Done

Executing the following commands:
  Install VAS Client (vasclnt)
  Install VGP Client (vasgp)
  License VAS (license)
  Join the Active Directory Domain (join)

Do you wish to continue? (yes|no)? [yes]: yes

Do you accept the Quest Software, Inc. agreement (yes|no) [no]: yes

Installation of <vasclnt> was successful.

Installation of <vasgp> was successful.

Would you like to install further licenses (yes|no)? [no]: yes
Please specify the full local path for each license file, e.g. 
/tmp/licenses/license1.txt.

Standard wildcards are also valid, e.g. /tmp/licenses/*.txt.

When all licenses have been installed press <enter> to quit.

Please specify full local path of license to install (<enter> to quit):
> /var/tmp/QAS-197-39181.txt
Installed '/var/tmp/QAS-197-39181.txt' --> '/etc/opt/quest/vas/licenses/QAS-197-39181.txt

Please specify full local path of license to install (<enter> to quit):

Resulting license state:
Number of Unix Enabled users in use: 0

---QAS---
Number of Licensed Unix Enabled Users: XXXX
Valid licenses: X
Number of days until license expires: XXXX

---QAS Siebel---
No licenses are installed.
Executing command: 'join'...

Do you wish to join the host to an Active Directory domain at this time (yes|no)? [yes]: yes

Checking whether computer is already joined to a domain ... no
Password for Administrator@EXAMPLE.COM: ADFPASSWORD
Stopping daemon: vasd ... OK
Configuring forest root ... example.com ... OK
Joining computer to the domain as hostquest.example.com ... OK
Joined using computer object "CN=quest,CN=Computers,DC=example,DC=com" ...
OK
Writing vas.conf ... OK
Populating misc cache ... OK
Applying Group Policy Settings ... OK
Starting daemon: vasd ... OK
Caching Schema... OK
Caching Users... OK
Mapping mapped users ... OK
Processing user overrides... OK
Caching Groups... OK
WARNING: No Unix-enabled groups found in domain!
Processing group overrides... OK
Caching Srvinfo... OK
Caching Netgroups... OK
Configuring Name Service Switch ... OK
Configuring PAM Authentication ... OK

In the preceding example, QAS agents were installed and a valid license was applied to the installation.

Any users who require access to both Oracle Solaris and Windows servers should have their UNIX account enabled on the Active Directory Server. Figure 2 shows creation of a Windows user named A N Test.

You can access this properties panel by selecting a user in the "Active Directory Users & Computers" application under the Administrator tools on the Active Directory domain controller.
Figure 2. Creating a test user called AN Test

Once you have created the user, you must enable the user for UNIX access, as shown in Figure 3.

Figure 3. Enabling UNIX access

In the preceding example, the Windows user AN Test is assigned the UNIX username antest, a UID of 80592, and the GID 1000. (The group unixusers has been created with a GID of 1000, so this user by default joins the group unixusers.)

For further details on the processes for initial configuration, consult the Quest Authentication Services Installation Guide.

Configuring the Oracle ZFS Storage Appliance for Active Directory and QAS

1. Using the browser user interface (BUI) of the Oracle ZFS Storage Appliance, ensure that the DNS configuration refers to the same DNS server as the Active Directory servers. As shown in
the following figure, access the DNS Configuration screen by selecting Configuration > Services > DNS.

![DNS Configuration Screen]

**Figure 4. Verifying DNS configuration**

2. Ensure that the clocks on the Oracle ZFS Storage Appliance and the Windows AD Servers are in sync.

On the BUI, select Configuration and Services and then click on NTP. Figure 5 shows the screen display that results. As the browser is running on the Windows Active Directory server (shown as Client Time in the following display), you can see that the clocks are in sync.

![NTP Configuration Screen]

**Figure 5. Verifying clock synchronization**

3. Next, request to join the AD by selecting Configuration > Services > Active Directory, as seen in Figure 6.
4. Select **JOIN DOMAIN** as shown in Figure 7.

5. Enter the details of a Domain Administrator user to enable the Oracle ZFS Storage Appliance to join the AD.

6. If you have successfully joined, you will see a display similar to Figure 9.
Figure 9. Successful AD join

If a message indicating 'access is denied' or 'the operating system cannot log on the user' displays and the username and password are correct, you may need to change the LAN Manager compatibility level to level 2.

Do this by selecting Configuration > Services > SMB as shown in Figure 10.

Figure 10. Configuring the LAN Manager compatibility level – 1

Change the LAN Manager compatibility level to 2 and click APPLY, as shown in Figure 11.
Figure 11. Configuring the LAN Manager compatibility level - 2

Once this has been completed, retry from step 3.

7. Configure the Mapping rules to be applied by selecting **Configuration > Services > Identity Mapping** as shown in Figure 12.

Figure 12. Selecting Identity Mapping

8. Ensure that the mapping mode is set to IDMU as shown in Figure 13. Click **APPLY** if it was changed.
Verifying Correct Operation

In order to test correct operation, a share called QUEST-test was configured on the Oracle ZFS Storage Appliance owned by user antest. Within this share is a folder called Secret which has all permissions removed except for the owner antest (the UNIX version name for A N Test), as can be seen in the following screenshot of the Windows properties display for the folder Secret. These folders were created on the Windows AD client on the share presented by the Oracle ZFS Storage Appliance also accessible by the Oracle Solaris server.

A text file was created in the directory Secret by user antest and a further non-restricted text file called Test Document.txt was created in the root directory of the QUEST-test share.
The following Oracle Solaris CLI session shows that the appropriate permissions applied on the Windows environment have successfully translated to the Solaris environment through the Identity Mapping and services provided by QAS.

login: antest
Password: <Windows AD Password>
Oracle Corporation SunOS 5.11 11.0 December 2011
antest@quest$ cd /net/zfssa/export/QUEST-test
antest@quest$ ls -alR
    total 16
   drwxr-xr-x+ 3 antest other 4 Feb 6 14:24 .
   drwxr-xr-x+ 4 root  root 255 Feb 6 14:21 ..
-dwx-------- 2 antest nobody 3 Feb 6 14:25 Secret
-rwxr--r-- 1 antest antest 26 Feb 6 14:10 Test Document.txt.txt
antest@quest$ ls -alR
   total 16
   drwxr-xr-x+ 3 antest other 4 Feb 6 14:24 .
   drwxr-xr-x+ 4 root  root 255 Feb 6 14:21 ..
-dwx-------- 2 antest nobody 3 Feb 6 14:25 Secret
-rwxr--r-- 1 antest antest 26 Feb 6 14:10 Test Document.txt.txt

antest@quest$ cd Secret
   bash: cd: Secret: Permission denied
antest@quest$ logout

Next, another AD UNIX-enabled user logs in to the Solaris server to view the share:

login: lookyloo
Password: <Windows AD Password>
Oracle Corporation SunOS 5.11 11.0 December 2011
lookyloo@quest$ cd /net/zfssa/export/QUEST-test
lookyloo@quest$ ls -alR
   total 13
   drwxr-xr-x+ 3 antest other 4 Feb 6 14:24 .
   drwxr-xr-x+ 4 root  root 255 Feb 6 14:21 ..
-rwxr-------- 1 antest nobody 82 Feb 6 14:26 My PIN Collection.txt
lookyloo@quest$ cd Secret
   bash: cd: Secret: Permission denied
lookyloo@quest$ logout

The correct permissions have therefore been applied in both environments.

Conclusion
The Oracle ZFS Storage Appliance Identity Mapping and Active Directory support provides an effective platform to share data between Oracle Solaris and Windows environments, with Quest Authentication Services being the single point of user account administration. Through QAS, restrictive permissions can be applied correctly in both environments to ensure data security.
# References

For more information, visit the following Web resources.

<table>
<thead>
<tr>
<th>Web Resource Description</th>
<th>Web Resource URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Solaris</td>
<td><a href="http://www.oracle.com/solaris">www.oracle.com/solaris</a></td>
</tr>
<tr>
<td>Quest Software</td>
<td><a href="http://www.quest.com">www.quest.com</a></td>
</tr>
<tr>
<td>Quest Authentication Services</td>
<td><a href="http://www.quest.com/authentication-services/">www.quest.com/authentication-services/</a></td>
</tr>
</tbody>
</table>