Oracle SolarisでQuest Authenticationを利用するためのSun ZFS Storage Applianceの構成方法

2012年5月
Andrew Ness著

この記事では、オラクルのSun ZFS Storage ApplianceでQuest Authentication Servicesを構成してOracle Solaris 10またはOracle Solaris 11環境をActive Directoryと統合する方法について説明します。

Quest SoftwareのQuest Authentication Services（QAS）は、WindowsベースのActive DirectoryとUNIX（Oracle Solaris 10およびOracle Solaris 11）やLinuxなどの他のプラットフォームの認証機能を統合できるクロス・プラットフォーム・ブリッジ機能を提供します。

QASをインストールして構成することにより、指定されたActive Directoryユーザーおよびグループがsolarisシステムで認識されるようになり、Active DirectoryユーザーやグループのsolarisのユーザーID（UID）またはグループID（GID）に対する一貫性が実現されます。また、Oracle Solarisホストが Active Directoryのパスワードを検証できるようになります。

Quest Authentication Servicesにより、UNIXユーザーとWindowsユーザーに対してActive Directoryによる一元管理が提供されるため、オラクルのSun ZFS Storage Applianceのストレージを共有する両方のプラットフォームに関して権限に一貫性を持たせることができます。

内容

概要

Active Directory（AD）を使用してユーザーおよびグループのディレクトリ・サービスを提供するには、ADのフレームワークで認証を実行する必要があります。ADにおける属性の構成のために、パスワード・フィールドは外部検証用にエクスポートされません。ADドメイン・サーバーだけが認証を提供できることから、Quest Authentication Servicesは、Windows以外のプラットフォームがActive Directoryに対して認証することを可能にするために必要なブリッジ機能を提供します。

また、QASは、Windowsの内部ユーザーおよびグループ識別子とOracle Solarisのユーザーおよびグループidのマッピングを提供します。このマッピングがSun ZFS Storage Applianceによって使用されることにより、異なるプラットフォーム間で一貫性のある権限とファイルの所有権が維持されます。

QASは、ADドメイン・コントローラにインストールされ、ADに必要な変更を加えて、Oracle Solarisクライアントにインストールされているエージェントが ADを使用できるようにします。Sun ZFS Storage Applianceへの追加のソフトウェア・パッケージのインストールは不要ですが、マッピング・プロセスを容易にするために、Sun ZFS Storage Applianceで構成変更が必要になる場合があります。

Sun ZFS Storage Appliance用にQASを有効化するプロセスには、2つのステップがあります。まず、ADサービスを通常の方法で使用できるようにSun ZFS Storage Applianceを構成する必要があります。次に、マッピング・サービスを構成して、協調して動作するすべてのプラットフォームで所有権および権限属性を共有できるようにします。

次の図は、Sun ZFS Storage ApplianceによるQASデプロイメントのアーキテクチャの例です。

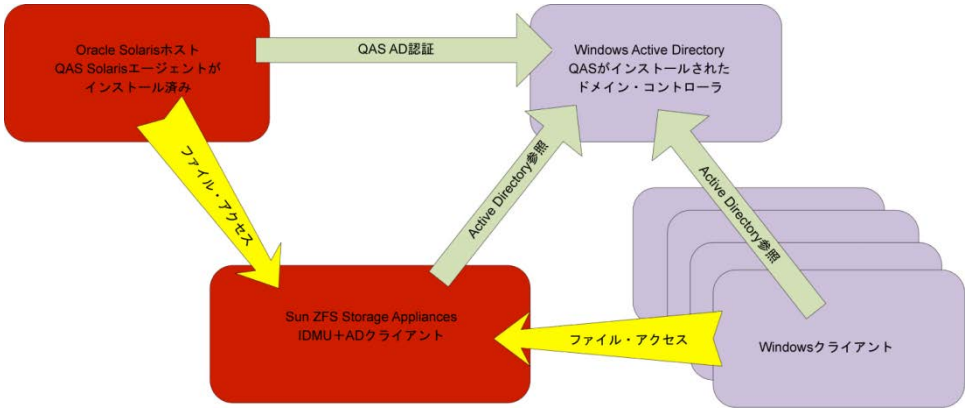


図1. Sun ZFS Storage ApplianceによるQASデプロイメント

Quest Authentication ServicesエージェントのOracle Solarisへのインストール

この項では、QASエージェントをOracle Solarisホスト・システムにインストールする手順の概要を示します。完全な手順および詳細については、*Quest Authentication Servicesのインストール・ガイド*（www.quest.com/authentication-services/）を参照してください。

1. Oracle Solarisホスト上のコマンドライン・インタフェース（CLI）セッションに接続します（telnet、ssh、またはコンソールを使用）。
2. Oracle Solarisサーバーにrootとしてログインするか、有効なユーザーとしてログインしてsuコマンドによりrootユーザー・ロールを割り当てます。
3. インストール・メディアとライセンス・キー・ファイルを確認します。

```
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/
[…]

root@quest# cd QAS-Agents
root@quest# ./install.sh

Quest Authentication Services Installation Script
Script Build Version: 4.0.3.24
Copyright 2011 Quest Software, Inc. ALL RIGHTS RESERVED.
Protected by U.S. Patent Nos. 7,617,501, 7,895,332, 7,904,949. Patents pending.

      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

Executing command: 'vasclnt'…
[…]
Do you accept the Quest Software, Inc. agreement (yes|no) [no]: yes
[…]
/opt/quest/share/oat/oat.msg
/opt/quest/share/oat/oat_adlookup.msg
/opt/quest/share/oat/oat_match.msg
/opt/quest/usr/lib/security/64/pam_vas3.so
/opt/quest/usr/lib/security/pam_vas3.so
[ verifying class <run> ]
## Executing postinstall script.
Registering vasd with SMF
WARNING: This system does not support a system wide global manpath.
You will need to set your MANPATH environment variable to /opt/quest/man,
or use "man -M /opt/quest/man <manpage>" to view the man pages.

Installation of <vasclnt> was successful.
vasclnt (4.0.3.24) installed.

Executing command: 'vasgp'...
echo 'y' | pkgadd -a '/tmp/vas-admin' -G -d '/home/admin/QAS-
Agents/client/solaris10-x64/vasgp_SunOS_5.10_i386-4.0.3.24.pkg' all
```

```
Processing package instance <vasgp> from </home/admin/QAS-
Agents/client/solaris10-x64/vasgp_SunOS_5.10_i386-4.0.3.24.pkg>

vasgp 4.0.3.24(amd64) 4.0.3.24
Copyright 2011 Quest Software, Inc. ALL RIGHTS RESERVED. Protected by U.S. Patent Nos.
7,617,501, 7,895,332, 7,904,949. Patents pending.
[…]
Installation of <vasgp> was successful.
vasgp (4.0.3.24) installed.

Executing command: 'license'...              Found existing licenses
Number of Unix Enabled users in use:           0

---QAS---
No licenses are installed.
---QAS Siebel---
No licenses are installed.

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:       XXXXX
Valid licenses:                              X
Number of days until license expires:        XXXXX

---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: ADPASSWORD
Stopping daemon: vasd ... OK
Configuring forest root ... example.com ... OK
```

```
Configuring site ... Default-First-Site-Name ... OK
Joining computer to the domain as host/quest.example.com ... OK
Joined using computer object "CN=quest,CN=Computers,DC=example,DC=com" ...
OK
Writing vas.conf ... OK
Populating misc cache ... OK
Preparing to apply Group Policy ... 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
```

この例では、QASエージェントがインストールされ、有効ライセンスがインストールに適用されています。

SolarisサーバーとWindowsサーバーの両方にアクセスする必要のあるユーザーは、Active Directoryサーバーで**UNIX**アカウントを有効にする必要があります。図2は、`ANTest`というWindowsユーザーの作成を示しています。

このプロパティ・パネルにアクセスするには、Active Directoryドメイン・コントローラの管理ツールに含まれている"Active Directoryユーザーとコンピューター"アプリケーションでユーザーを選択します。

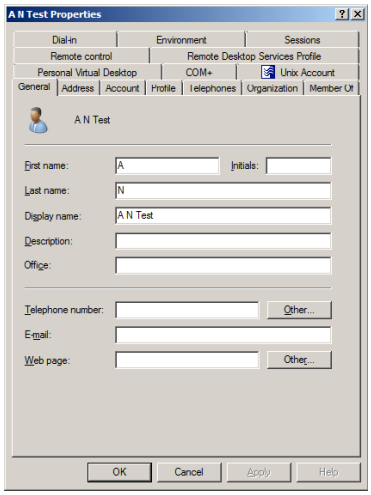


Figure 2. **A N Test**というテスト・ユーザーの作成

ユーザーを作成したら、ユーザーのUNIXアクセスを有効にする必要があります（図3を参照）。

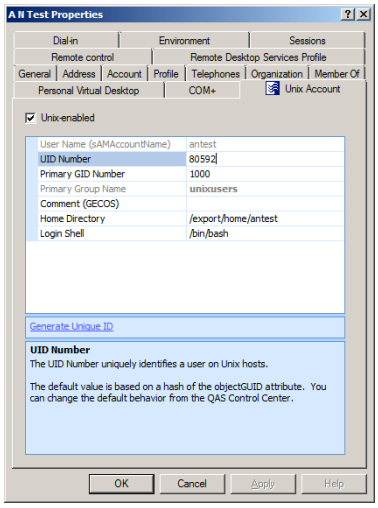


図3. UNIXアクセスの有効化

この例では、Windowsユーザー**A N Test**にUNIXユーザー名**antest**、UID80592、GID1000が割り当てられています（グループ**unixusers**がGID1000で作成されているため、このユーザーはデフォルトで**unixusers**グループに追加されます）。

初期構成のプロセスの詳細については、*Quest Authentication Services*のインストール・ガイドを参照してください。

Active DirectoryおよびQASに関するSun ZFS Storage Applianceの構成

1. Sun ZFS Storage Applianceのブラウザ・ユーザー・インタフェース（BUI）を使用して、DNS構成がActive Directoryサーバーと同じDNSサーバーを参照していることを確認します。次の図のように、「Configuration」→「Services」→「DNS」を選択してDNS構成画面にアクセスします。

図4. DNS構成の確認

2. Sun ZFS Storage ApplianceとWindows ADサーバーの時計が同期していることを確認します。

   BUIで、「Configuration」→「SERVICES」を選択し、「NTP」をクリックしてください。図5に示す画面が表示されます。ブラウザはWindows Active Directoryサーバー上で動作しているため（次の図のClient Time）、時計が同期していることを確認できます。

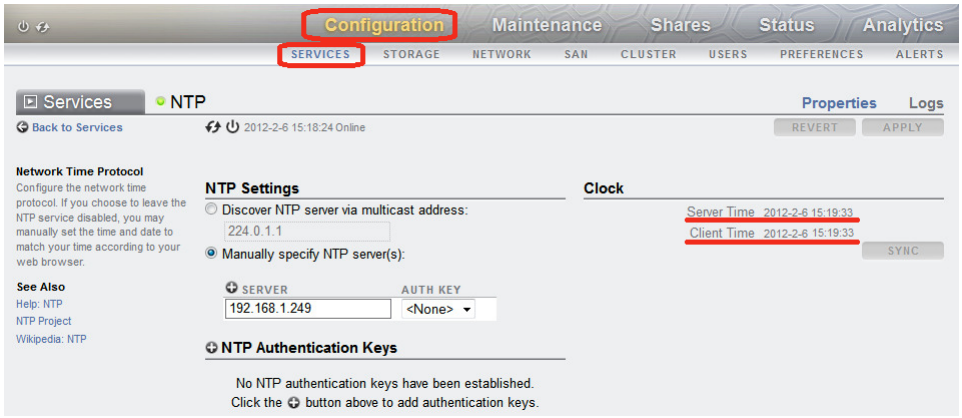


図5. 時計の同期の確認

3. 次に、「Configuration」→「Services」→「Active Directory」を選択してADへの参加を要求します（図6を参照）。

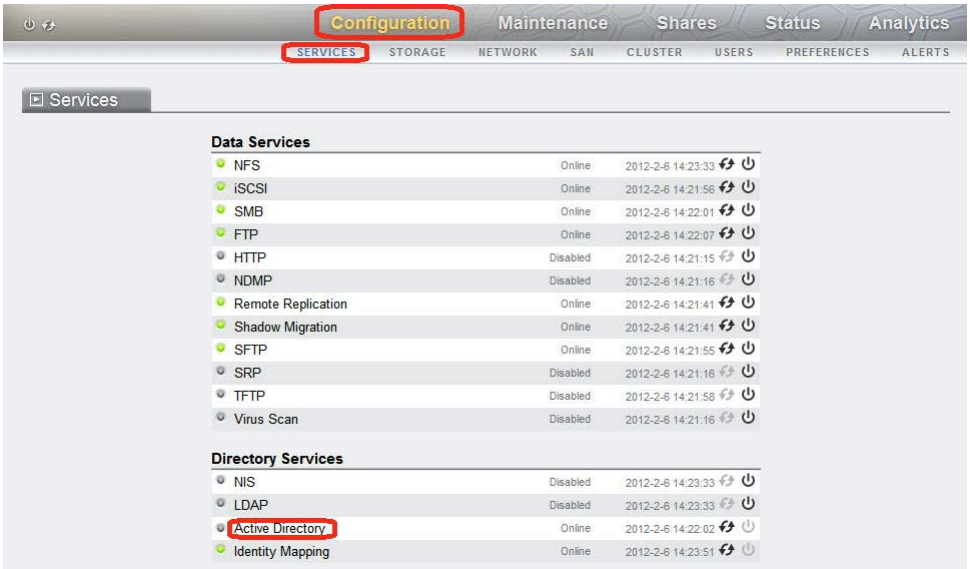


図6. Active Directoryの選択

4. 「JOIN DOMAIN」を選択します（図7を参照）。

図7. JOIN DOMAINの選択

5. ドメイン管理者ユーザーの詳細情報を入力して、ADに参加させるSun ZFS Storage Appliance を有効にします。

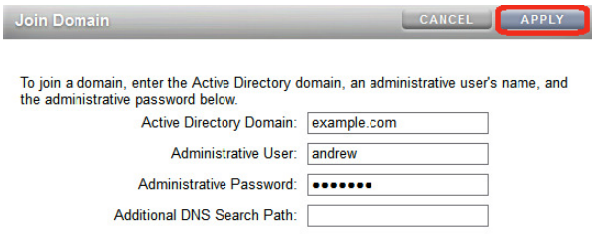


図8. AD管理者の詳細情報の入力

6. 正常に参加すると、図9のような画面が表示されます。

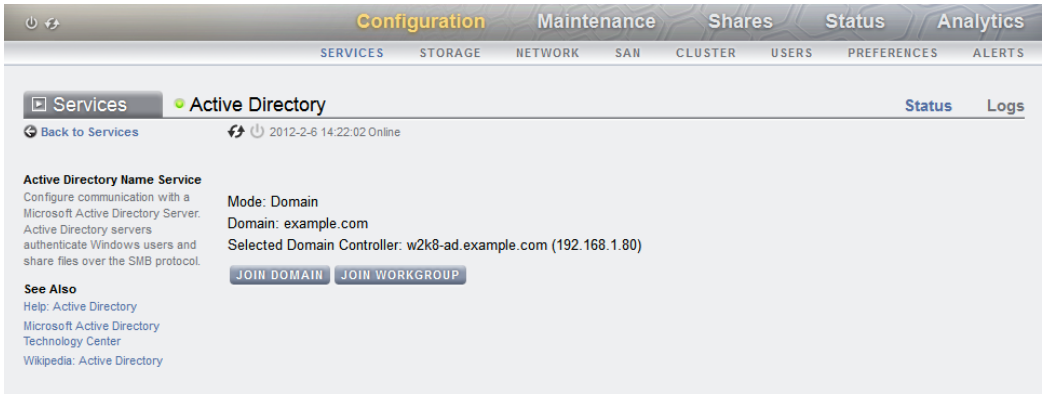


図9. ADへの正常な参加

'アクセスが拒否された'または'オペレーティング・システムがユーザーをログオンできない'ことを示すメッセージが表示されるが、ユーザー名とパスワードが正しい場合は、LAN Managerの互換性レベルをレベル2に変更する必要があります。

これを実行するには、「Configuration」→「Services」→「SMB」を選択します（図10を参照）。

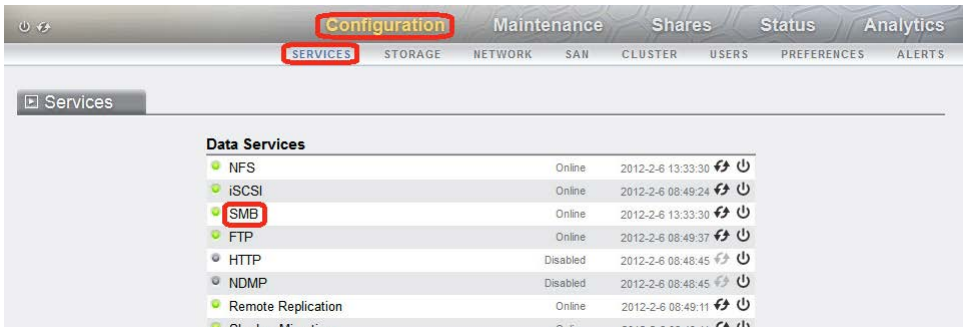


図10. LAN Managerの互換性レベルの構成（1）

LAN Managerの互換性レベルを2に変更して、「APPLY」をクリックします（図11を参照）。

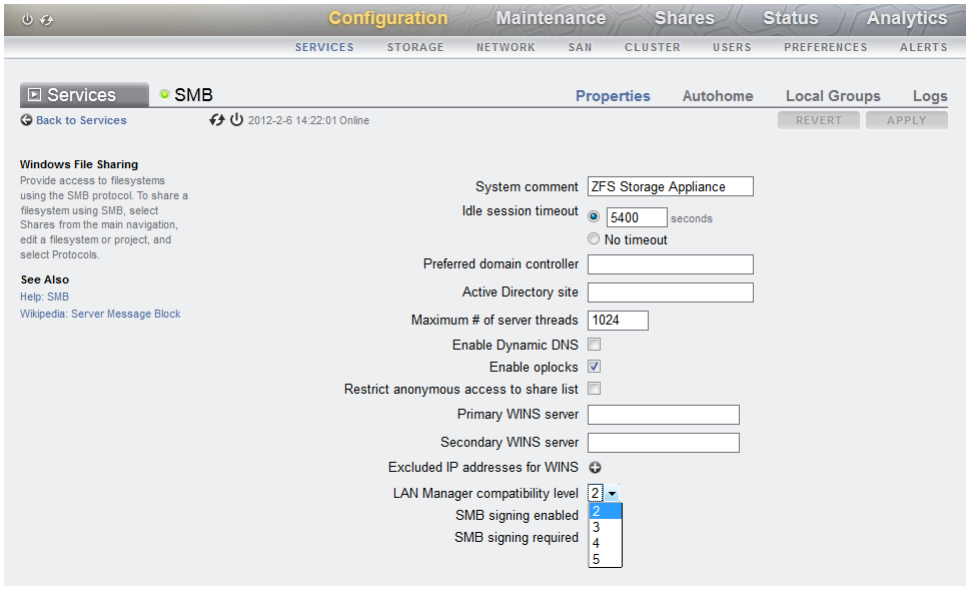


図11. LAN Managerの互換性レベルの構成（2）

この手順が完了したら、手順3からやりなおしてください。

7. 「Configuration」→「Services」→「Identity Mapping」を選択して、適用するマッピング・ルールを構成します（図12を参照）。

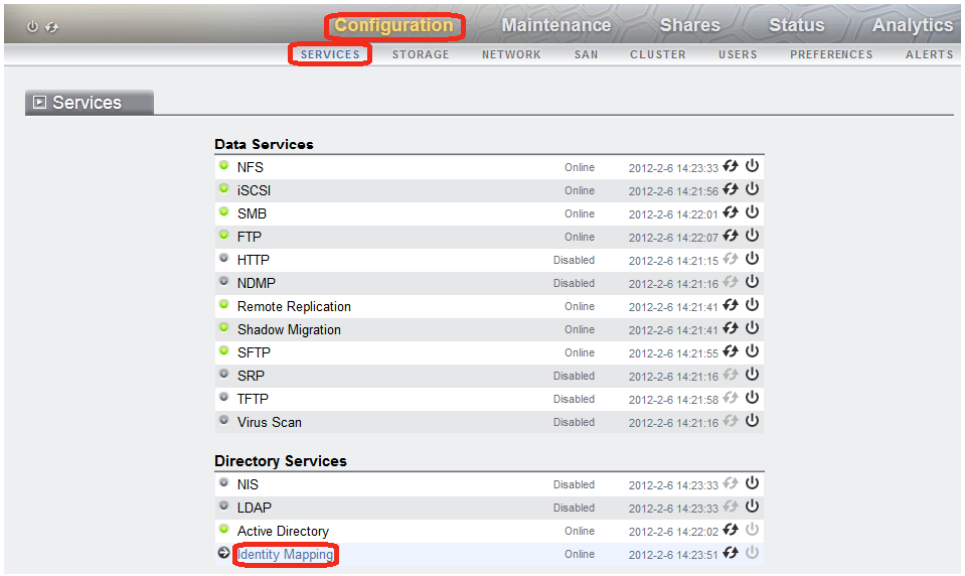
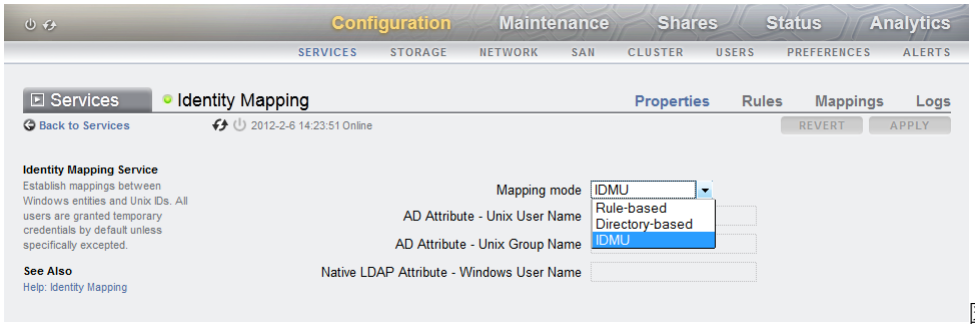


図12. Identity Mapping（IDマッピング）の選択

8. マッピング・モードがIDMUになっていることを確認します（図13を参照）。変更した場合は「Apply」をクリックしてください。



13. マッピング・モードIDMUの選択

正常な動作の確認

正常に動作することを確認するために、ユーザー`antest`が所有するSun ZFS Storage Appliance上に`QUEST-test`という共通フォルダが構成されています。この共有フォルダ内には、所有者`antest`（`A N Test`のUNIXバージョンのユーザー名）以外のすべての権限が削除された`Secret`というフォルダがあります。`Secret`フォルダのWindowsプロパティのスクリーンショットが次のように表示されます。これらのフォルダは、Windows ADクライアント上の、Sun ZFS Storage Applianceによって提供される共有フォルダに作成されており、Oracle Solarisサーバーからもアクセスできます。

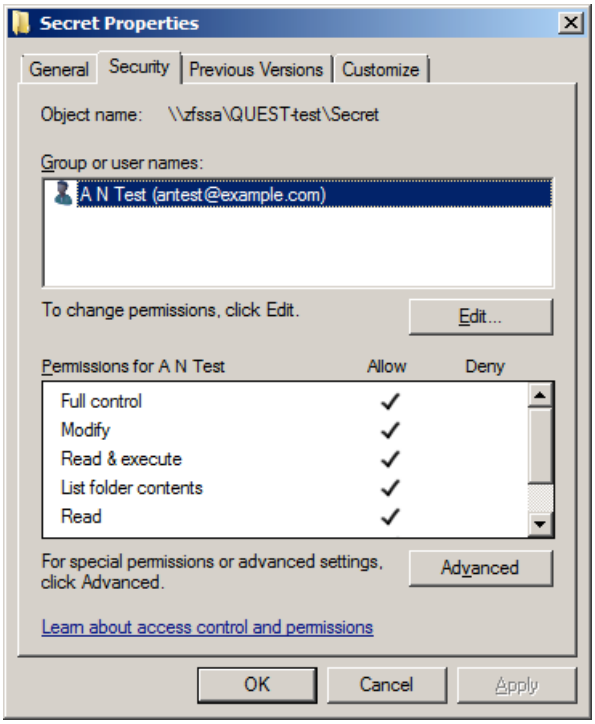


図14. `QUEST-test¥Secret`の制限された権限

テキスト・ファイルが`antest`ユーザーによって`Secret`ディレクトリに作成されており、さらに、制限のないテキスト・ファイル（`Test Document.txt`）が`QUEST-test`共有フォルダのrootディレクトリに作成されています。

次のSolaris CLIセッションは、Windows環境で適用されている適切な権限が、IDマッピングとQASによって提供されるサービスにより、Solaris環境に正常に変換されたことを示しています。

```
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 ..
drwx------+ 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 ..
drwx------+ 2 antest   nobody    3 Feb 6 14:25 Secret
-rwxr--r--  1 antest   antest   26 Feb 6 14:10 Test Document.txt.txt

./Secret:
total 8
drwx------+ 2 antest   nobody    3 Feb 6 14:25 .
drwxr-xr-x+ 3 antest   other     4 Feb 6 14:24 ..
-rwx------+ 1 antest   nobody   82 Feb 6 14:26 My PIN Collection.txt
antest@quest$ logout
```

次に、別のAD UNIX対応ユーザーでSolarisサーバーにログインして、共有フォルダを表示します。

```
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
.:
./Secret:Permission denied
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--r--  1 antest   antest   26 Feb 6 14:10 Test Document.txt.txt
lookyloo@quest$ cd Secret
-bash: cd: Secret: Permission denied
lookyloo@quest$ logout
```

このようにして、正しい権限が両方の環境で提供されていることを確認できます。

結論

Sun ZFS Storage ApplianceのIDマッピングとActive Directoryのサポートにより、ユーザー・アカウントの一元管理を実現するQuest Authentication Servicesを使用することで、Solaris環境とWindows環境の間でデータを共有するための効果的なプラットフォームが提供されます。QASにより、制限された権限を両方の環境で適切に適用できるため、データのセキュリティが確保されます。

参考資料

詳細情報については、次のWebリソースを参照してください。

Webリソースの説明	**WebリソースのURL**
Oracle Solaris	http://www.oracle.com/jp/products/servers-storage/solaris/solaris11/overview/index.html
Quest Software	http://www.quest.com
Quest Authentication Services	http://www.quest.com/authentication-services/
Oracle Sun ZFS Storage Appliances	http://www.oracle.com/jp/products/servers-storage/storage/nas/overview/index.html