# 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

<u>Quest Authentication ServicesエージェントのOracle Solarisへのインストール</u> Active DirectoryおよびQASに関するSun ZFS Storage Applianceの構成 正常な動作の確認 結論 参考資料

## 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。

- 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
---0AS---
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:
                                             Х
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 \ldots 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、AN Test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。

N Test Properties		?.
Dial-in	Environment	Sessions
Remote contro	I Remote	Desktop Services Profile
Personal Virtual D General Address / A	esktop COM+	Unix Account
🔏 A N Test		
Eirst name:	A	Initials:
Last name:	N	
Digplay name:	A N Test	
Description:		
Offige:	[	
Telephone number:		<u>O</u> ther
E- <u>m</u> ail:		
Web page:		Other
	OK Cancel	Apply Help

#### 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)。

	uc.s				
Dial-in	Î	Environr	ment	Se	ssions
Remote	control	Î I	Remote Desk	top Services	Profile
eneral Addre	ss Account I	Profile	Telephones	Organization	h Í Member Of
Personal Vi	tual Desktop		COM+	😽 Uni	x Account
🔽 Unix-enabl	ed				
User Name	(sAMAccountN	lame) a	antest		
UID Numbe	er	8	30592		
Primary GI	D Number	3	1000		
Primary Gr	oup Name		unixusers		
Comment (	GECOS)				
Home Direct	tory	1	export/home	e/antest	
Louis Chall					
Login Shell		/	/bin/bash		
Login Shell		/	/bin/bash		
Generate Uni	que ID	/	/bin/bash		
Generate Uni UID Numbe The UID Num The default v can change th	r r ber uniquely ide alue is based or he default beha	n a hash o avior from 1	bin/bash iser on Unix H f the objectC the QAS Con	nosts. SUID attribute Irrol Center.	s. You

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

 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。

0 #		Confi			iance	Shar	es	Status A	nalytics
		SERVICES	STORAGE	NETWORK	SAN	CLUSTER	USERS	PREFERENCES	ALERTS
E Services	DNS							Properties	Logs
G Back to Services	<b>€\$</b> () 20	12-2-6 08:49:28 Online						REVERT	APPLY
Domain Name Service DNS is used to map host name such as oracle com to their corresponding IP addresses. Is is always erabled on your appliance, and can be configu manually or based on your cu DHCP settings. In addition, you elect to attempt hostname resolution using other director services (if configured).	ss DNS red rrent i may Y		Allow IPv4 Allow IPv6	DNS Dom DNS Serve non-DNS resolut 6 non-DNS resolut	ain exa (s) O ion V ion V	ample.com	80		
See Also Help: DNS									

#### 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。

U 43	Cont	iguration	Mainte	enance	Shar	es	Status	Analytics
	SERVICES	STORAGE	NETWORK	SAN	CLUSTER	USERS	PREFERENCE	S ALERTS
Services • NT	P						Propert	ties Logs
G Back to Services		13					REVERT	APPLY
Network Time Protocol Configure the network time	NTP Settings			Clo	ck			
protocol. If you choose to leave the NTP service disabled, you may	O Discover NTP server via i	multicast address	:			Server Time	2012-2-6 15:19:33	-
manually set the time and date to	224.0.1.1					Client Time	2012-2-6 15:19:33	
match your time according to your web browser.	Manually specify NTP set	erver(s):						SYNC
See Also	SERVER	AUTH KEY						
Help: NTP	192.168.1.249	<none></none>	•					
Wikipedia: NTP	ONTP Authentication	Keys						
	No NTP authentication Click the 😳 button abo	i keys have been we to add authent	established. ication keys.					

#### 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)。

_	Gornigara	Maintenanoe		
	SERVICES STOR	AGE NETWORK SAN	CLUSTER USERS	PREFERENCES
ces				
	Data Services			
	NFS	Online	2012-2-6 14:23:33 🗲 🙂	
	iSCSI	Online	2012-2-6 14:21:56 🗲 🔱	
	SMB	Online	2012-2-6 14:22:01 🗲 🔱	
	FTP	Online	2012-2-6 14:22:07 🗲 🔱	
	• HTTP	Disabled	2012-2-6 14:21:15 🖅 😃	
	NDMP	Disabled	2012-2-6 14:21:16 🖅 😃	
	Remote Replication	Online	2012-2-6 14:21:41 🗲 🙂	
	Shadow Migration	Online	2012-2-6 14:21:41 🗲 🙂	
	SFTP	Online	2012-2-6 14:21:55 🗲 🙂	
	© SRP	Disabled	2012-2-6 14:21:16 🖅 😃	
	TFTP	Disabled	2012-2-6 14:21:58 € එ Ů	
	Virus Scan	Disabled	2012-2-6 14:21:16 🕩 😃	
	Directory Services			
	© NIS	Disabled	2012-2-6 14:23:33 <b>€∌ Ů</b>	
	C LDAP	Disabled	2012-2-6 14:23:33 🖅 😃	
	Active Directory	Online	2012-2-6 14:22:02 🗲 🕛	
	Identity Mapping	Online	2012-2-6 14:23:51 🔂 🕛	

図6. Active Directoryの選択

4. 「JOIN DOMAIN」を選択します(図7を参照)。

⊎ #	Conf	iguration	Mainte	enance	Shar	es	Status	A	nalytics
	SERVICES	STORAGE	NETWORK	SAN	CLUSTER	USERS	PREFER	ENCES	ALERTS
E Services • Ac	tive Directory								Status
G Back to Services	↔ · · · · · · · · · · · · · · · · · · ·	ed							
Active Directory Name Service Configure communication will a Microsoft Active Directory Server. Active Directory servers authenticate Windows users and share files over the SMB protocol.	Mode: Workgroup Workgroup: Lavemill JOIN DOMAIN JOIN WOR	RKGROUP							
See Also Help: Active Directory									
Microsoft Active Directory Technology Center									
Wikipedia: Active Directory									

### 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。

Join Domain	CANCEL
To join a domain, enter the Active Directory d the administrative password belcw.	omain, an administrative user's name, and
Active Directory Domain:	example.com
Administrative User:	andrew
Administrative Password:	•••••
Additional DNS Search Path:	

## 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。

U 49	Cor	figuration	Mainte	enance	Shar	es	Status	An	alytics
	SERVICES	STORAGE	NETWORK	SAN	CLUSTER	USERS	PREFEREN	ICES	ALERTS
Services Ac Back to Services	tive Directory	le					5	Status	Logs
Active Directory Name Service Configure communication with a Microsoft Active Directory Server. Active Directory servers authenticate Windows users and share files over the SMB protocol. See Also Help: Active Directory Microsoft Active Directory Technology Center Wikipedia: Active Directory	Mode: Domain Domain: example.com Selected Domain Controlle JOIN DOMAIN JOIN WO	r: w2k8-ad.exam DRKGROUP	ple.com (192.16	68.1.80)					

## 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)。

0 33	Confi	iguration	Mainte	enance	Shar	es	Status	Analytics
	SERVICES	STORAGE	NETWORK	SAN	CLUSTER	USERS	PREFERENCE	ES ALERTS
Services								
	Data Services							
	NFS			Online	2012-2-6 13:33	:30 € 0		
	iSCSI			Online	2012-2-6 08:49	24 分 心		
	SMB			Online	2012-2-6 13:33	:30 <b>€9 (</b> )		
	FTP			Online	2012-2-6 08:49	37 分 也		
	• HTTP			Disabled	2012-2-6 08:48	:45 €€ 🙂		
	© NDMP			Disabled	2012-2-6 08:48	45 分 心		
	Remote Replication			Online	2012-2-6 08:49	11 好也		
						CA (I)		

### 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)。

0 &	Confi	guration	Mainte	enance	Shares	Status A	Analytics
	SERVICES	STORAGE	NETWORK	SAN C	LUSTER USERS	PREFERENCES	ALERTS
Services SMB G Back to Services	好 (J) 2012-2-6 14:22:01 Online			Properti	ies Autohome	Local Group	s Logs
Windows File Sharing Provide access to filesystems using the SMB protocol. To stare a filesystem using SMB, select Shares from the main navigation, edit a filesystem or project, and select Protocols. <b>See Also</b> Help: SMB Wikipedia: Server Message Block	Restri	Preferr Maximur E ict anonymous F Sec Excluded IP LAN Manag S S	System com Idle session tin red domain cont Active Directory m # of server thr nable Dynamic Enable opl access to shar Primary WINS s condary WINS s addresses for V er compatibility SMB signing end SMB signing red	ment ZFS Stu heout © 5400 No tir roller v site meads 1024 DNS locks Ø re list lerver lerver level 2 abled 3 yuired 4 5	orage Appliance 0 seconds meout		

## 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)。

0 7	Confi	guration	Mainte	nance	Shar	es	Status	Analytics
	SERVICES	STORAGE	NETWORK	SAN	CLUSTER	USERS	PREFERENCES	ALERTS
Services								
	Data Services							
	NFS			Online	2012-2-6 14:23	33 <b>€≯ (</b> )		
	iSCSI			Online	2012-2-6 14:21	:56 <b>€</b> ∮ (J		
	SMB			Online	2012-2-6 14:22	:01 <b>チチ</b> 也		
	FTP			Online	2012-2-6 14:22	o7 🗲 U		
	HTTP		0	Disabled	2012-2-6 14:21	15 €∌ 也		
	NDMP		[	Disabled	2012-2-6 14:21	<sub>16</sub> €∌ ப்		
	Remote Replication			Online	2012-2-6 14:21	41 <b>€9</b> Ů		
	Shadow Migration			Online	2012-2-6 14:21	·41 <b>チナ</b> し		
	SFTP			Online	2012-2-6 14:21	:55 <b>€9 (</b> )		
	SRP		0	Disabled	2012-2-6 14:21	16 €୬ 🖒		
	TFTP		0	Disabled	2012-2-6 14:21	58 €≯ U		
	Virus Scan		[	Disabled	2012-2-6 14:21	:16 €∌ U		
	Directory Services							
	NIS		0	Disabled	2012-2-6 14:23	:33 €∌ Ů		
	LDAP		0	Disabled	2012-2-6 14:23	33 €୬ ଓ		
	Active Directory			Online	2012-2-6 14:22	02 <b>69</b> 也		
	Identity Mapping			Online	2012-2-6 14:23	51 <b>69</b> 也		

## 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。

0 4	Confi	guration	Mainte	nance	Shares	s Sta	atus Ar	alytics
	SERVICES	STORAGE	NETWORK	SAN	CLUSTER	U SER S	PREFERENCES	ALERTS
Services • Ident	ity Mapping				Properties	Rules	Mappings	Logs
G Back to Services	🗲 🕛 2012-2-6 14:23:51 Online						REVERT	APPLY
Identity Mapping Service Establish mappings between Windows entities and Unix Ds. All users are granted temporary credentials by default unless specifically excepted.		AD Attribu AD Attribute	Mapping r te - Unix User N e - Unix Group N	node ID ame Di ame Di	MU ule-based rectory-based MU			
See Also Help: Identity Mapping	Native LDA	P Attribute -	Windows User N	ame				

### 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。

Secret Properties				2
General Security Prev	ious Versions C	ustomize	1	
Object name: \\zfssa	QUEST-test\Se	cret		
<u>G</u> roup or user names:				
A N Test (antest@e	example.com)			
To change permissions,	click Edit.		<u>E</u> dit	
Permissions for A N Test		Allow	Deny	
Full control		~		-
Modify		~		
Read & execute		~		
List folder contents		~		
		/		_
Read		~		<b>T</b> I
For special permissions of	or advanced settin	ngs,	Ad <u>v</u> anced	
For special permissions of click Advanced.	or advanced setti	ngs,	Ad <u>v</u> anced	
For special permissions of click Advanced.	or advanced settin	ngs,	Ad <u>v</u> anced	

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 ..
                   antest 26 Feb 6 14:10 Test Document.txt.txt
-rwxr--r-- 1 antest
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