An Oracle White Paper
February 2011

Sun ZFS Storage Appliance Rule-Based Identity Mapping Between Active Directory and Network Information Services Implementation Guide

Introduction

The Sun ZFS Storage Appliance identity mapping service manages users of both Active Directory services and Network Information Services (NIS) by associating the Windows and UNIX identities of each user. This allows shares, such as directories or files to which access is controlled by a password, to be exported and accessed by clients using either Common Internet File System (CIFS)/Server Message Block (SMB) or Network File system (NFS) protocols.

This document describes a rule-based mapping approach in which rules are created to map identities by name. These rules establish correlations between Windows and UNIX identities. While this document uses NIS as a directory service for UNIX identities, a lightweight Directory Access Protocol (LDAP) server can provide the same function.

Overview and Prerequisites

This document describes how to configure the Sun ZFS Storage Appliance identity mapping service and related appliance settings required for rule-based identity mapping to work properly. It describes the activities that take place on the appliance and demonstrates how the mappings work on both Windows and Solaris clients.

The content of this document is based on the Sun ZFS Storage Appliance Software Release 2010.Q3. Although previous versions of the Sun ZFS Storage Appliance software referred to SMB as CIFS, for the purposes of this paper, the CIFS service is referred to as SMB.

This document assumes the reader has a working knowledge of Windows Active Directory and Solaris NIS environments.

The procedures in this document assume that:

- The Sun ZFS Storage Appliance has been initially configured with a network setup including an IP address, netmask, and gateway
- The appliance clock is in sync with the Network Time Protocol (NTP) time server.
- A storage pool has been configured
- Each domain is populated with users and groups to be mapped

The user and group permission settings are shown with default values and are not intended to imply a best practice.

For a more information about the Sun ZFS Storage Appliance identity mapping service, including concepts, functions, and behaviors, see the section ***Error! Reference source not found.*** at the end of this paper.

This document does not cover:

- Domain Name System (DNS)/NTP setup on domain controllers
- Directory-based identity mapping
- Identity Management for UNIX (IDMU) integration
- Deny mappings
- Unidirectional mappings Active Directory-to-UNIX or UNIX-to-Active Directory)
- Autohome features

Preparing the Sun ZFS Storage Appliance

The network and name services must be configured appropriately for the identity mapping service to function properly. This section describes the non-default appliance settings required to configure rule-based identity mapping between Active Directory and NIS.

Setting Up DNS Services

Before the Sun ZFS Storage appliance can be joined to the Active Directory domain, the DNS Services settings must be set appropriately. On the DNS Services page:

- Enter the domain name of the DNS server in the **DNS Domain** box.
- Enter the IP address of the DNS server in the **DNS Server(s)** box.
- Click the **APPLY** button.

Additional DNS servers can be added by clicking the **+ icon**.

Specifying the NTP Server

Although it is not required, using the Active Directory server as the NTP server ensures that the appliance clock is in sync with the Active Directory domain clock. Joining the appliance to the Active Directory domain may fail if the time difference between the domain controller and the appliance is more than five minutes.

On the NTP Services page:

- Select the option Manually specify NTP servers(s).
- In the **Server** box, enter the NTP server name.
- Click the **APPLY** button.

Additional NTP servers can be added by clicking the **+ icon**.

NOTE: Selecting the **Sync** button synchronizes the appliance time to the browser time, but not to the NTP server time.

Joining the Appliance to the Active Directory Domain

To join the appliance to an Active Directory domain, on the Active Directory Services page:

- Click the **JOIN DOMAIN** button.
- Enter the Active Directory Domain and the Administrative User and Password.
- Click the **APPLY** button.

If an authentication failure occurs while attempting to join the domain, see the section Troubleshooting SMB Services below for troubleshooting information.

Joining the Appliance to the NIS Domain

Before joining the appliance to the NIS domain, ensure that a record exists for the NIS server in DNS. This is required for proper name resolution to take place on the appliance. On the NIS Services page:

- Enter the NIS domain name in the **Domain** box.
- Select the option **Use listed servers** and enter the server name in the box that appears below the option.
- Click the **APPLY** button.

Additional NIS slaves can be added by clicking the **+ icon**.

Troubleshooting SMB Services

If an error message is displayed that states that *access is denied* or that *the operating system cannot log on the user*, and you have entered the correct user name and password, you may need to change the **LAN Manager Compatibility Level** setting. The authentication modes supported on the Sun ZFS Storage appliance are LAN Manager (LM), NT LAN Manager (NTLM), LMv2, and NTLMv2.

For help configuring SMB services, click on the Help button at the upper right corner in the appliance interface. On the left sidebar, select **Services**. In the Contents box at the right, select **Data**. In the table that is displayed, select **SMB**.

Configuring Active Directory Services on Windows Server 2003 and 2008

For updated information about how to configure the Active Directory services to work with different versions of Windows Server, click on the Help button at the upper right corner in the appliance interface. On the left sidebar, select **Services**. In the Contents box at the right, select **Directory.** In the table that is displayed, select **Active Directory**. In the Contents box at the right, select **Windows Server 2008 Support**.

For SMB troubleshooting information, see the topic Cannot Join a Windows Domain on the CIFS Service Troubleshooting page in the Genunix OpenSolaris wiki.

Troubleshooting NFS Services

In some previous versions of the Sun ZFS Storage software, when the appliance is joined to an Active Directory domain, the Active Directory domain becomes the first option in the NFS Services **search** field. As a result, the NFSv4 identity domain defaults to the Active Directory domain.

To override this behavior, on the NFS Services page:

- Unselect the option **Use DNS domain as NFSv4 identity domain**.
- Enter the preferred NFSv4 identity domain name into the **Use custom NFSv4 identity domain** box.
- Click the **APPLY** button.

NOTE: If the identity domain differs between an NFSv4 client and the server, the client will not be able to authenticate successfully.

Defining Rule-Based Identity Mappings

This section describes setting up mapping rules that allow Active Directory and UNIX identities to be mapped using bi-directional mappings. These rules represent the most common deployment of identity mapping and are sufficient for most customer environments that rely solely on rule-based identity mapping.

NOTE: Changes to the identity mapping rules may not take immediate effect, so may not affect active file sharing sessions. To avoid confusion, configure the mappings before exporting the shares. If a change is necessary while clients are accessing a share, go to the Mappings tab and flush the cache of mappings to force all clients to reestablish mappings.

Selecting the Mapping Mode

To select the mapping mode, on the Services page:

- Select **Rule-based** from the **Mapping mode** dropdown box, as shown in Figure 1.
- Click the **APPLY** button.

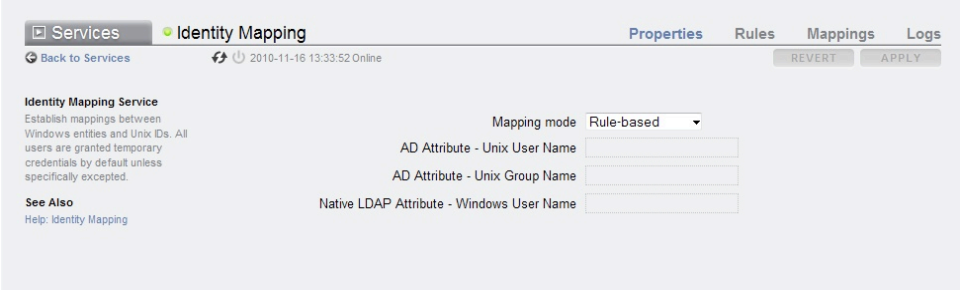

Figure 1: Identity Mapping properties

Adding Rule-Based Mappings Using Domain-Wide Rules

A domain-wide mapping rule matches some or all of the names in a Windows domain to UNIX names.

NOTE: Only one bi-directional mapping that maps all users in the Windows domain to all UNIX users is allowed for each Windows domain.

The Windows-to-UNIX mapping is case sensitive. For example, the Windows user name *jsmith* matches the UNIX user name *jsmith*, but the Windows user name *Jsmith* does not match. An exception can be made by using the wildcard character (*) to map multiple user names.

To create a domain-wide mapping rule for users:

- Click the **+ icon** on the Rules tab next to the word **Rules**.
- Select the options shown in Figure 2.

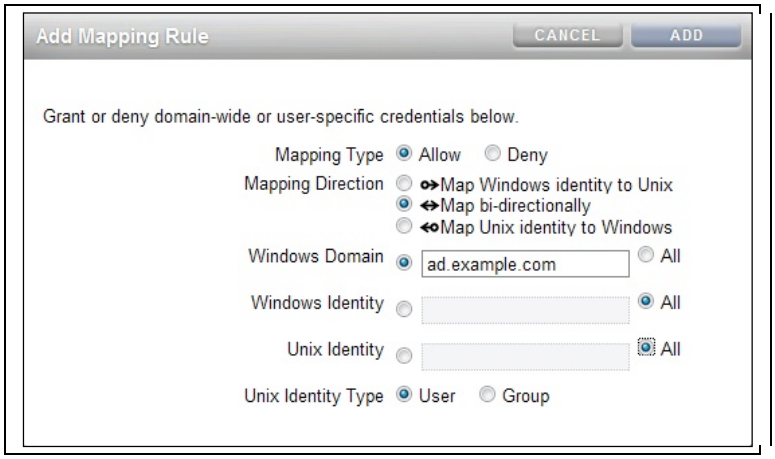

Figure 2: Adding domain-wide user mapping

To create a domain-wide mapping rule for groups:

- Click the **+ icon** on the Rules tab next to the word **Rules**.
- Select the options shown in Figure 3.

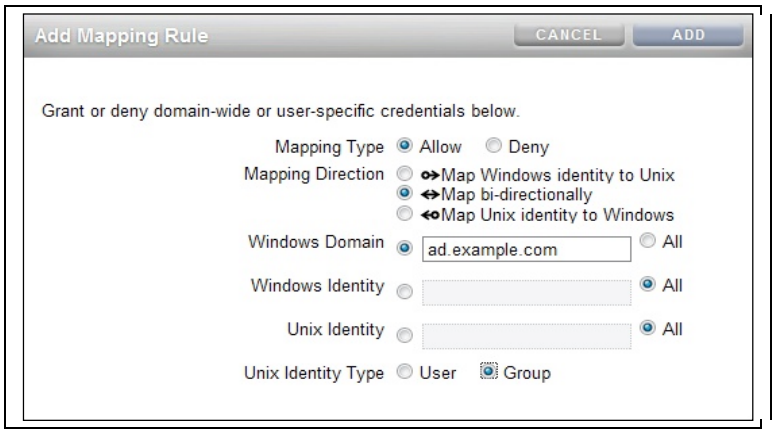

Figure 3: Adding a domain-wide group mapping rule

Figure 4 shows the results of the two mapping rules created in Figure 2 and Figure 3.

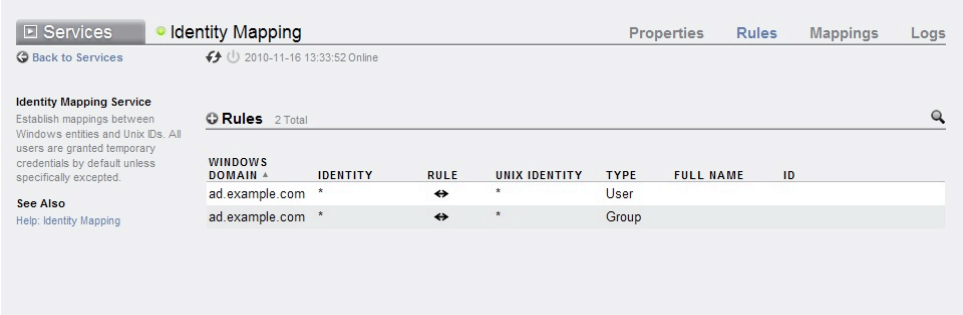

Figure 4: Summary of domain-wide rules

Figure 5 and Figure 6 show how users and groups are mapped based on the domain-wide rules created above. If a Windows User or Group name is entered in the **Identity** field and a mapping has been defined, the corresponding UNIX user or group name and ID are displayed under User Properties. Likewise, if a UNIX User or Group name is entered in the **Identity** field and a mapping has been defined, the corresponding Windows user or group name and ID are displayed under User Properties.

Figure 5 shows the Windows user *user01* mapped to the UNIX user *user01*.

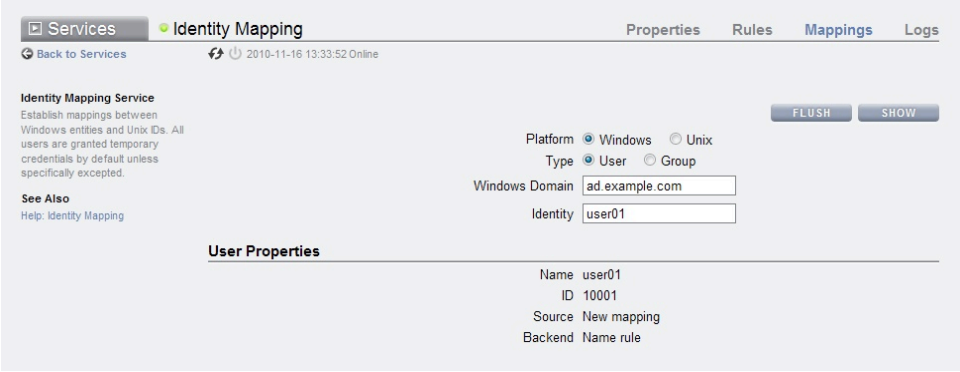

Figure 5: Domain-wide mapping results for Windows user *user01*

Figure 6 shows the UNIX group *group01* mapped to the Windows group *group01@ad.example.com*.

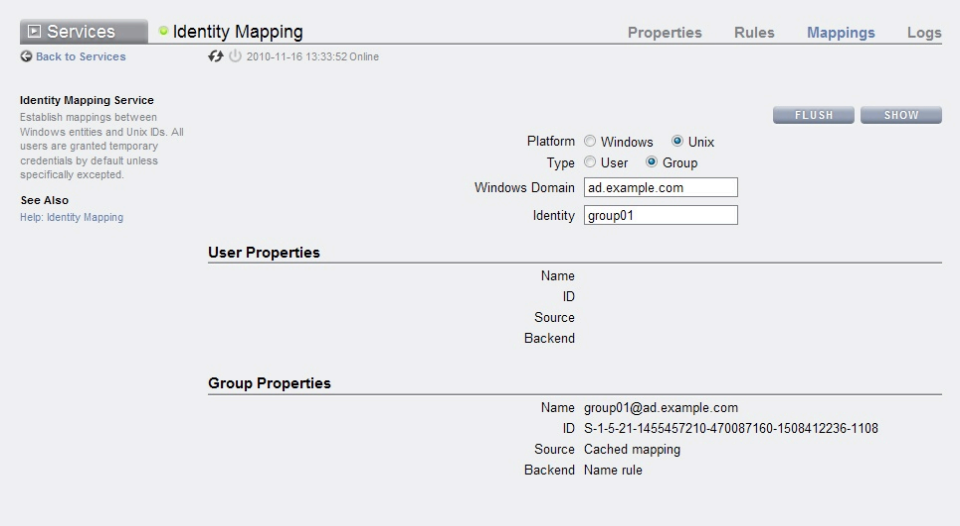

Figure 6: Domain-wide mapping results for UNIX group *group01*

Adding Rule-Based Mappings for an Individual User or Group

To create a mapping rule between the Windows user *ad-user* and UNIX user *nis-user*:

- Click the **+ icon** on the Rules tab next to the word **Rules**.
- Select the options shown in Figure 7.

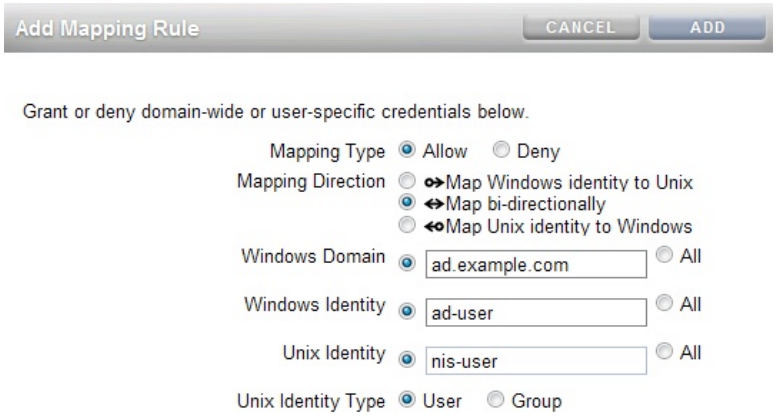

Figure 7: Adding an individual user rule

To create a mapping rule between the Window group *ad-group* and UNIX group *nis-group*:

- Click the **+ icon** on the Rules tab next to the Work Rules.
- Select the options shown in Figure 8.

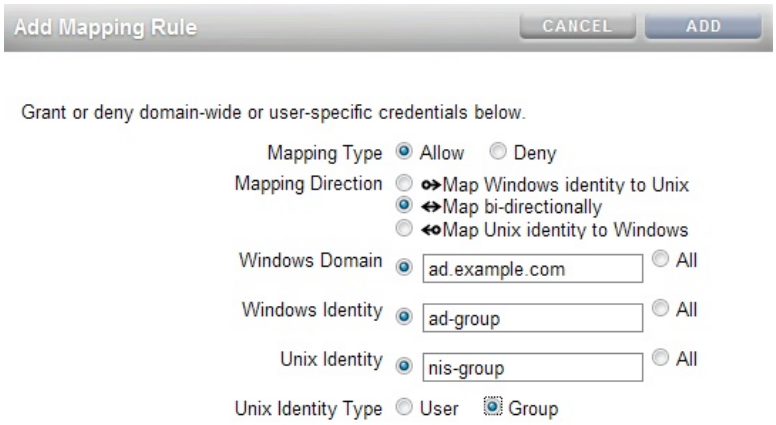

Figure 8: Adding an individual group rule

To create a mapping rule to map the Active Directory default group *Domain Users* to the NIS default group *staff*:

- Select the **+ icon** on the Rules tab next to the word **Rules**.
- Select the options shown in Figure 9.

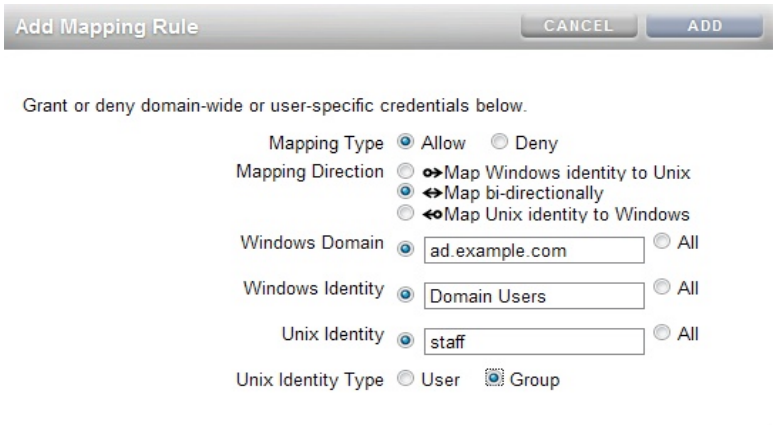

Figure 9: Adding a default group rule

The Rules page shown in Figure 10 lists the user and group mapping rules defined in Figure 7, Figure 8, and Figure 9.

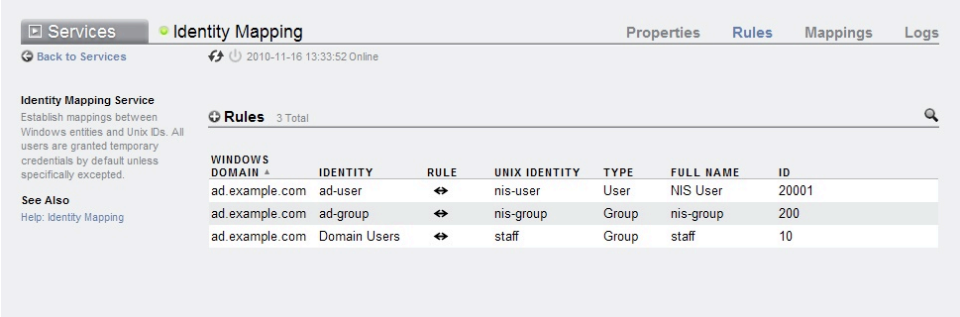

Figure 10: Summary of individual user and group rules

Figure 11 shows the Windows user *ad-user* mapped to the UNIX user *nis-user* as a result of the Individual User rule defined in Figure7.

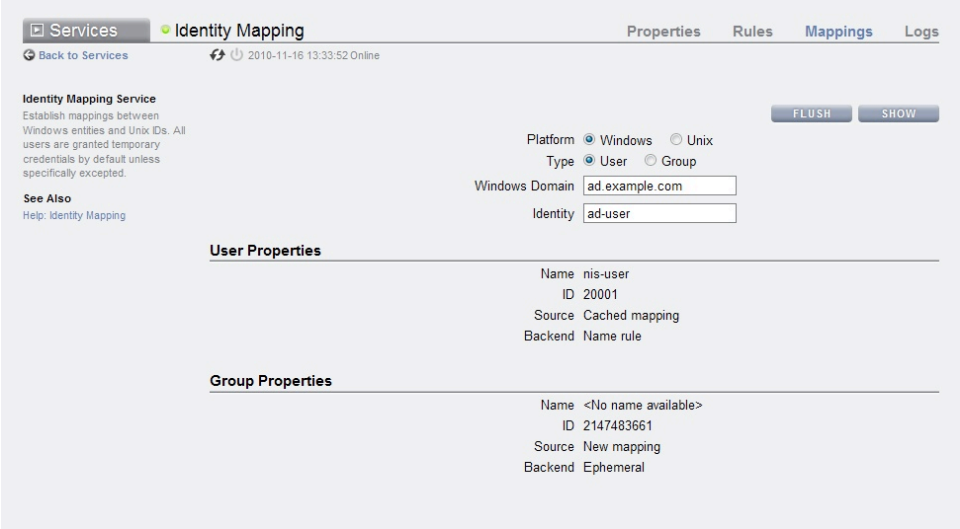

Figure 11: Individual user mapping results

Figure 12 shows the UNIX group *nis-group* mapped to the Windows group *ad-group@ad.example.com* as a result of the Group rule defined in Figure 8.

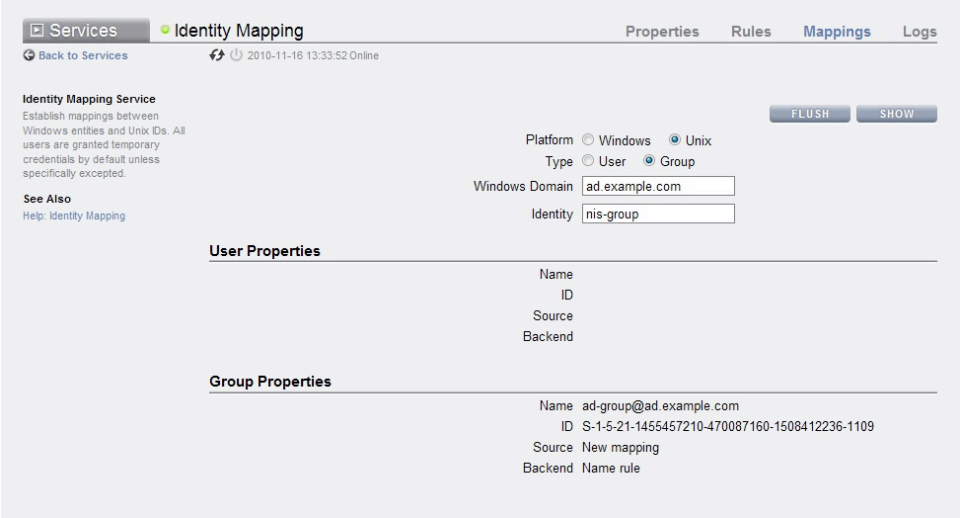

Figure 12: Individual group mapping results

Figure 13 shows the UNIX group *staff* mapped to the Windows group *Domain Users@ad.example.com* as a result of the Default Group rule defined in Figure 9.

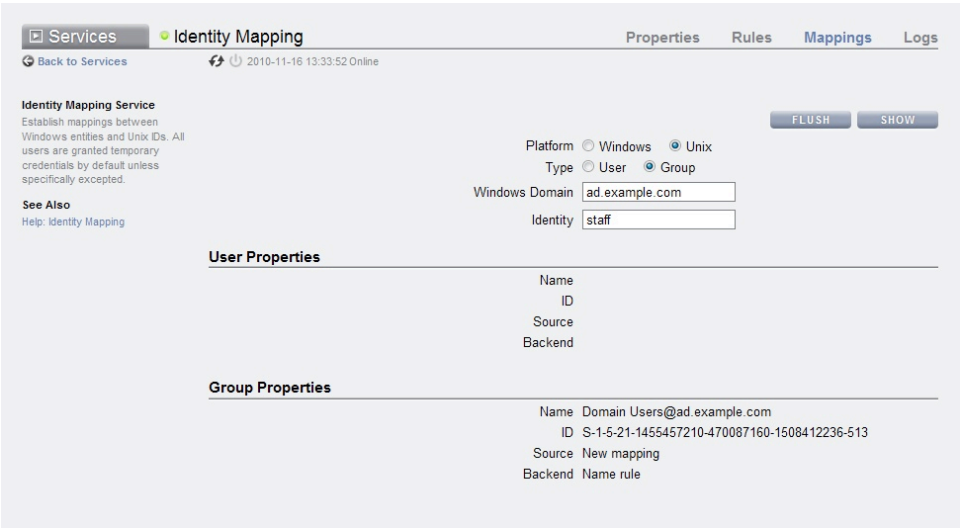

Figure 13: Default group mapping results

Using Domain-Wide and Individual Rule-Based Mappings Together

Domain-wide rules may not be sufficient if a user or group in the Active Directory domain does not have the same name in the NIS domain. For example, one might want to map the Active Directory *Domain Users* group to the NIS *staff* group.

The rules shown in Figure 14 include both domain-wide and individual mappings. When a request is made to map a Windows identity to a UNIX identity, the request is evaluated first in the context of all individual rules (the third, fourth, and fifth rules in Figure 14), then in the context of domain-wide rules (the first two rules in Figure 14). For this example, if the identity mapping service is asked to provide a UNIX identity for the Windows user *ad-user*, the service provides the UNIX user *nis-user* even if the service is also able to resolve a UNIX user named *ad-user*.

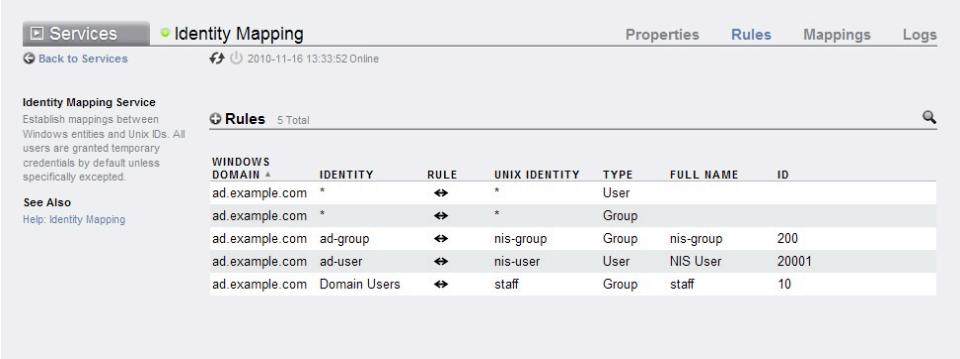

Figure 14: Summary of domain-wide and individual rules

Configuring and Assigning Shares

For rule-based identity mapping to function properly, shares must be configured with specific properties as described below. Shares can be created and configured at a user level or a group level.

Setting Up a User Share

This section describes how to create a user share, assign a user to the share, and set the share-level protocol and access settings.

Creating a User Share

To create a share named *user01_share* for the user *user01*:

- Select the default project in the Shares tab
- Select **Filesystems** and click the **+ icon**. The **Create Filesystem** page shown in Figure 15 is displayed.
- Enter the share name *user01_share* in the **Name** box, the user name *user01* in the **User** box, and the group name *staff* in the **Group** box.
- Under Permissions, select the option **Use Windows default permissions**.
- Click the **APPLY** button.

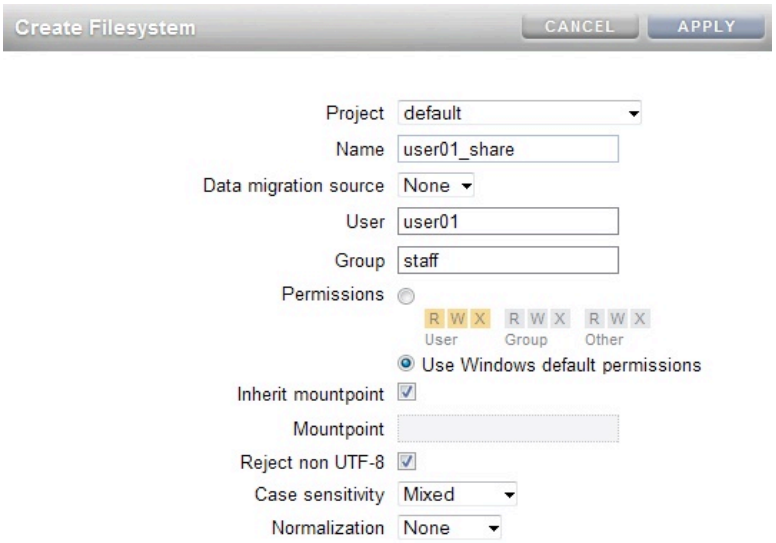

Figure 15: Creating a user share

Configuring User Share-Level Protocol Settings

To set up the SMB protocol at the user level for exporting a share, complete the steps below (see Figure 16).

On the Protocol tab for the share:

- Uncheck the **Inherit from project** checkbox.
- In the **Resource Name** box, replace the entry **off** with the entry **on**.
- Click the **APPLY** button.

The **Resource Name** is the name by which SMB clients refer to this share. The resource name set to **off** indicates no SMB client may access the share. The resource name set to **on** indicates the share is exported as `\\server\<filesystem_name>`. To specify a share name manually, enter a custom resource name other than ***on*** or ***off***.

If access-based enumeration is desired, it can be enabled by selecting the option **Enable Access-based Enumeration**. Access-based enumeration filters directory entries based on the credentials of the client. When the client does not have access to a file or directory, that file is omitted from the list of entries returned to the client. This option is not enabled by default.

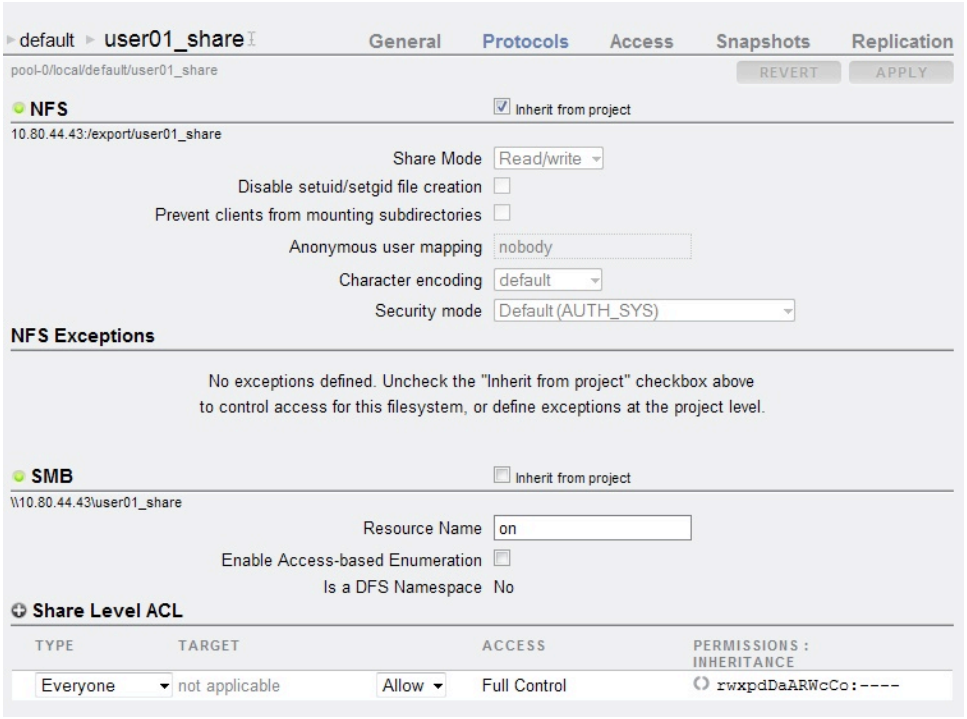

Figure 16: User share-Level SMB protocol settings

Configuring User Share-Level Access Settings

Access to the `root` directory is set when the share is created (see Creating a User Share) based on the permissions set at that time. This section describes the inheritance behavior for the access control list (ACL) in the Sun ZFS Storage Appliance Software Release 2010.Q3 and Software Release 2010.Q1. The examples in this section are based on a share *user01_share* assigned to the user *user01* that was mapped using domain-wide rules in section Adding Rule-Based Mappings Using Domain-Wide Rules.

ACL Behavior in the Sun ZFS Storage Appliance Software Release 2010.Q3

In the Software Release 2010.Q3, to set ACL behavior:

- Uncheck the **Inherit from project** checkbox.
- In the **ACL inheritance behavior** dropdown box, select **Inherit all entries**, as shown in Figure 17. When the **Inherit all entries** option is selected, all inheritable ACL entries are inherited. This option sets the ACL *passthrough* mode so that when a user creates a new file, the file inherits the permissions of the directory tree in which it is created. An administrator sets the permissions to be used for the ACL inheritance, such 0664 or 0666.
- Click the **APPLY** button.

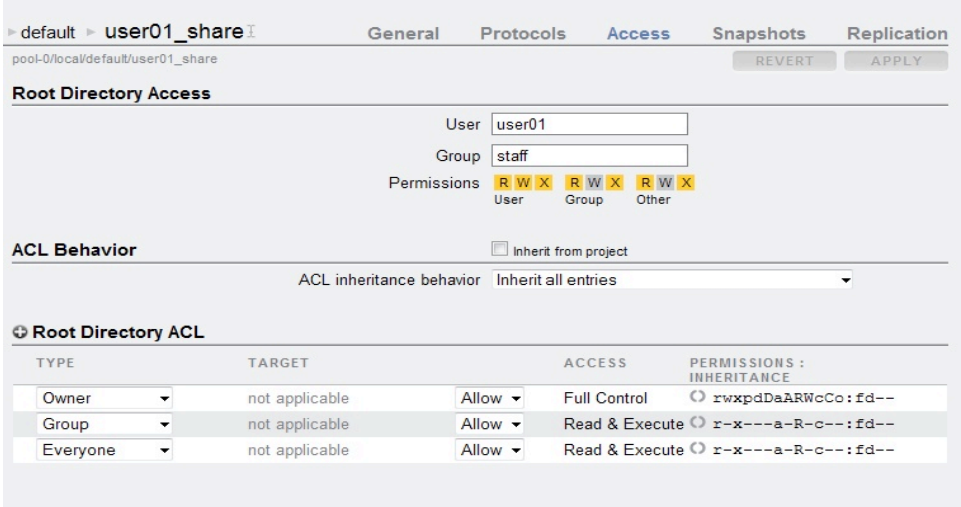

Figure 17: ACL inheritance behavior for Sun ZFS Storage Appliance Software Release 2010.Q3

The **Root Directory ACL** is set when the share is created based on the **Use Windows default permissions** option selected (see Figure 15). Figure 17 shows the three **Allow** mode entries that are created: one for Owner, one for Group, and one for Everyone.

To delete an entry, mouse over the entry and select the trash can icon.

To edit an entry, mouse over the entry and select the pencil editing icon.

To add an entry, click the **+ icon**.

After making changes, click the **APPLY** button.

ACL Behavior in Sun ZFS Storage Appliance Software Release 2010.Q1

In Software Release 2010.Q1, to set ACL behavior:

- Uncheck the **Inherit from project** checkbox, as shown in Figure 18
- In the **ACL behavior on mode change** drop down box, select **Do not change ACL** to preserve ACL entries when permission change operations are applied.
- In the **ACL inheritance behavior** drop down box, select **Inherit all entries** to indicate that all inheritable ACL entries are inherited.
- Click the *APPLY* button.

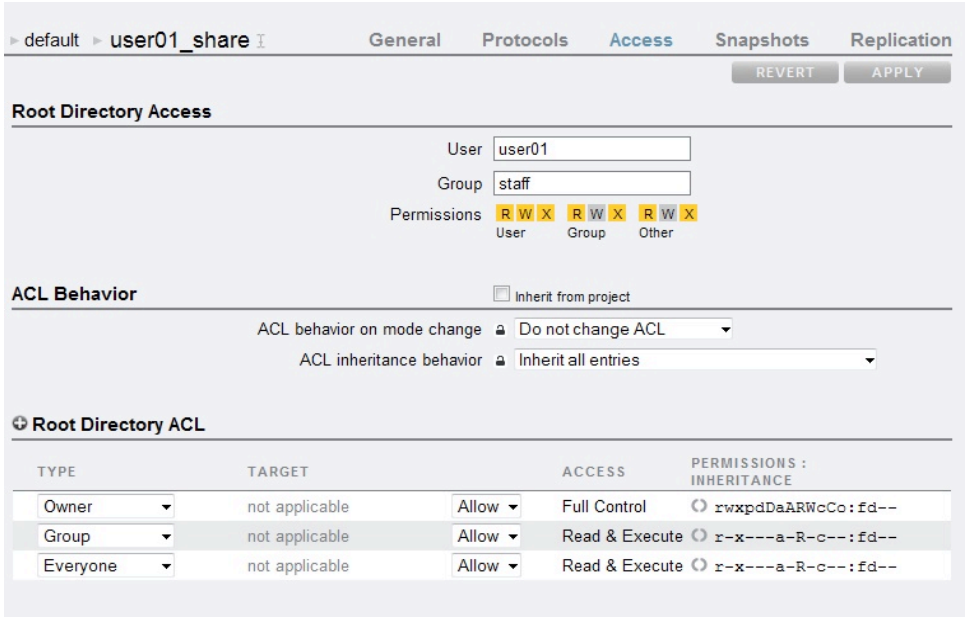

Figure 18: ACL inheritance behavior for Sun ZFS Storage Appliance Software Release 2010.Q1

The **Root Directory ACL** is set when the share is created based on the **Use Windows default permissions** option selected (see Figure 15). Figure 18 shows the three **Allow** mode entries that are created: one for Owner, one for Group, and one for Everyone.

To delete an entry, mouse over the entry and select the trash can icon.

To edit an entry, mouse over the entry and select the pencil editing icon.

To add an entry, click the **+ icon**.

After making changes, click the **APPLY** button.

Setting Up a Group Share

This section describes how to create a group share, assign a group to the share, and set the share-level protocol and access settings.

Creating a Group Share

To create a share called *group01_share* for the group *group01*:

- In the Shares tab, select the default project.
- Select **Filesystems** and click the **+ icon**. The Create Filesystem page is displayed (see Figure 19).
- Enter the share name *group01_share* in the **Name** box, a user name such as *root* in the **User** box, and the group name *group01* in the **Group** box.
- Under Permissions, select the option **Use Windows default permissions**.
- Click the **APPLY** button.

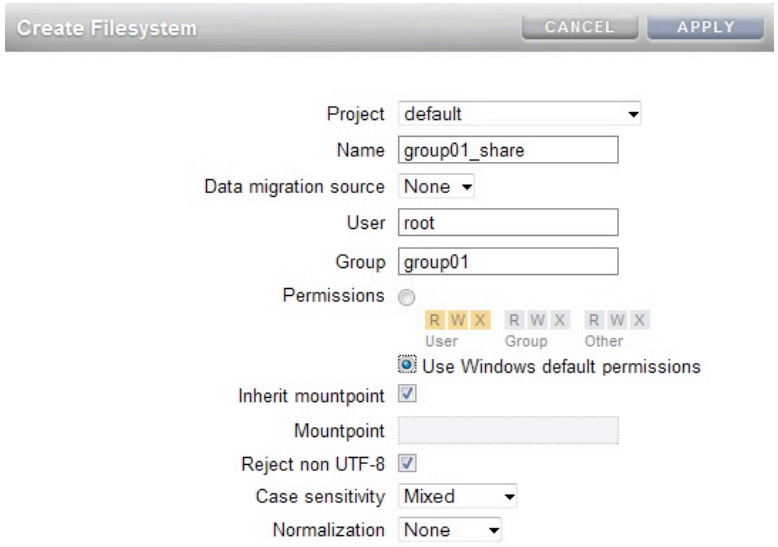

Figure 19: Creating a group share

Configuring Group Share-Level Protocol Settings

To set up the SMB protocol at the group level for exporting a share, complete the steps below (see Figure 20).

On the Protocol tab for the share:

- Uncheck the **Inherit from project** checkbox.
- In the **Resource Name** box, replace the entry **off** with the entry **on**.
- Click the **APPLY** button.

The **Resource Name** is the name by which SMB clients refer to this share. The resource name set to **off** indicates no SMB client may access the share. The resource name set to **on** indicates the share is exported as `\\server\<filesystem_name>`. To specify a share name manually, enter a custom resource name other than ***on*** or ***off***.

If access-based enumeration is desired, it can be enabled by selecting the option **Enable Access-based Enumeration**. Access-based enumeration filters directory entries based on the credentials of the client. When the client does not have access to a file or directory, that file is omitted from the list of entries returned to the client. This option is not enabled by default.

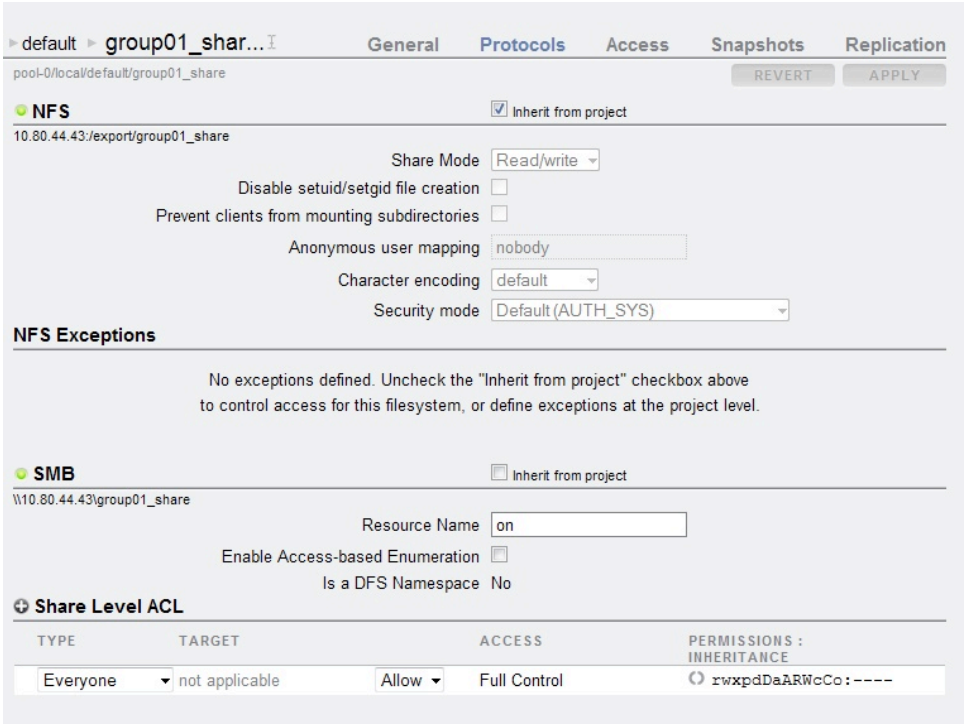

Figure 20: Group share-level SMB protocol settings

Configuring Group Share-Level Access Settings

This section describes how to create shares, assign groups to the shares, and set the share-level protocol and access settings.

Access to the `root` directory is set when the share is created (see Creating a User Share) based on the permissions set at that time. This section describes the inheritance behavior for the access control list (ACL) in the Sun ZFS Storage Appliance Software Release 2010.Q3 and Software Release 2010.Q1. The examples in this section are based on a share *group01_share* assigned to the group *group01* that was mapped using domain-wide rules.

ACL Behavior in Software Release 2010.Q3

In the Software Release 2010.Q3, to set ACL behavior:

- Uncheck the **Inherit from project** checkbox.
- In the **ACL inheritance behavior** dropdown box, select **Inherit all entries**, as shown in Figure 21. When the **Inherit all entries** option is selected, all inheritable ACL entries are inherited. This option sets the ACL *passthrough* mode so that when a user creates a new file, the file inherits the permissions of the directory tree in which it is created. An administrator sets the permissions to be used for the ACL inheritance, such 0664 or 0666.
- Click the **APPLY** button.

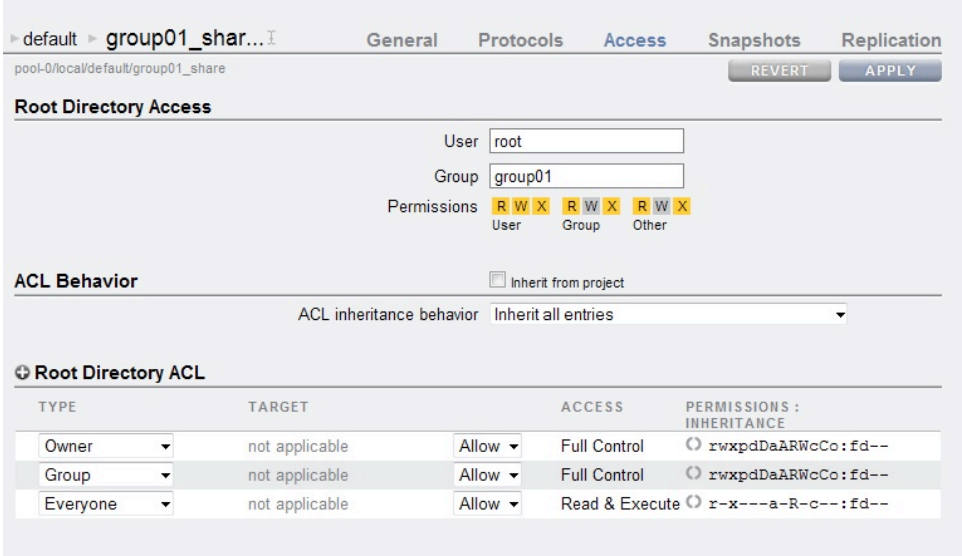

Figure 21: Group share-level access settings in Software Release 2010.Q3

The **Root Directory ACL** is set when the share is created based on the **Use Windows default permissions** option selected (see Figure 19). Figure 21 shows the three **Allow** mode entries that are created: one for Owner, one for Group, and one for Everyone.

To delete an entry, mouse over the entry and select the trash can icon.

To edit an entry, mouse over the entry and select the pencil editing icon.

To add an entry, click the **+ icon**.

After making changes, click the **APPLY** button.

Because this is a group share, full access may be granted to the group. To modify the **Root Directory ACL** for the group:

- Mouse over the ACL entry and select the pencil editing icon.
- To set the ACL entry to full control, on the Edit ACL Entry page, select **Full Control** from the dropdown box at the top of the page as shown in Figure 22.
- Click the **OK** button.

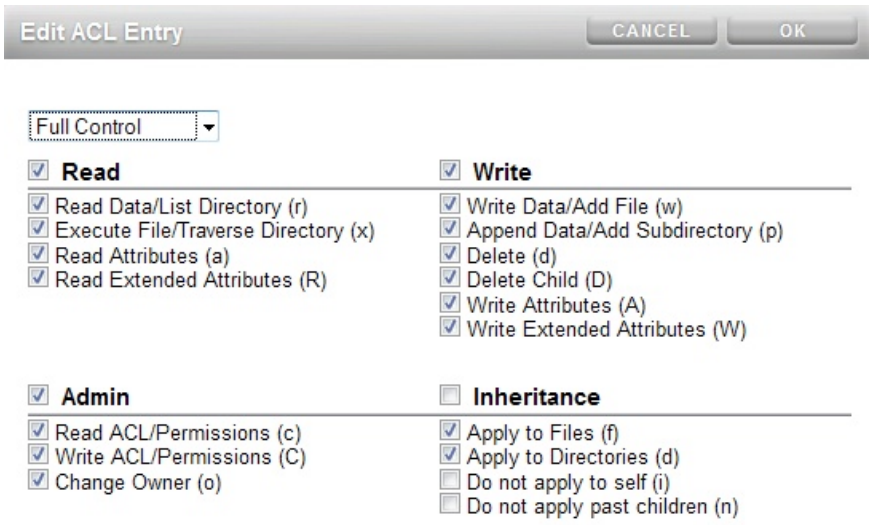

Figure 22: Editing the group ACL entry

ACL Behavior in Software Release 2010.Q1

In Software Release 2010.Q1, to set ACL behavior:

- Uncheck the **Inherit from project** checkbox, as shown in Figure 23.
- In the **ACL behavior on mode change** drop down box, select **Do not change ACL** to preserve ACL entries when permission change operations are applied.
- In the **ACL inheritance behavior** drop down box, select **Inherit all entries** to indicate that all inheritable ACL entries are inherited.
- Click the *APPLY* button.

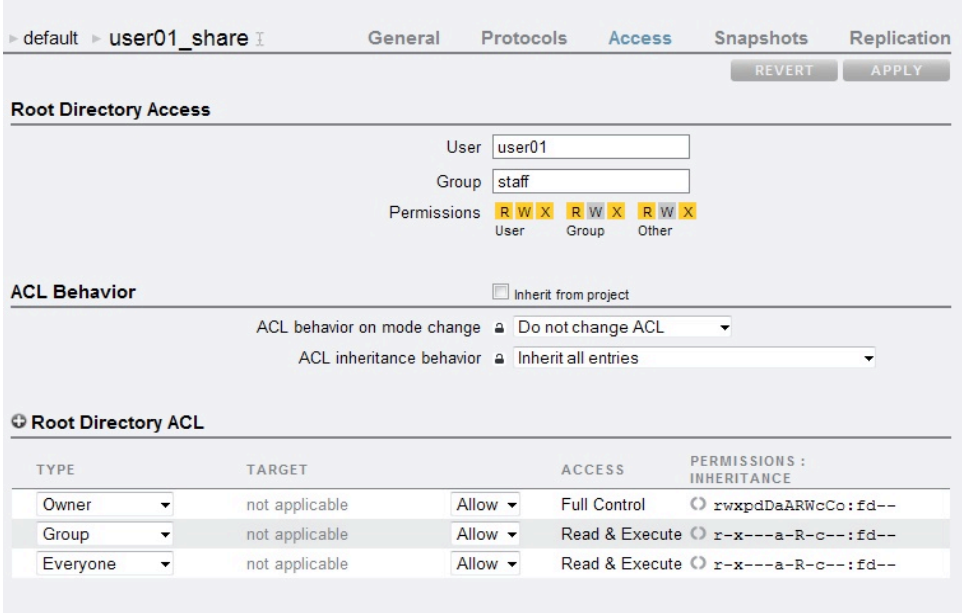

Figure 23: Group share-level access settings in Software Release 2010.Q1

The **Root Directory ACL** is set when the share is created based on the **Use Windows default permissions** option selected (see Figure 19). Figure 23 shows the three **Allow** mode entries that are created: one for Owner, one for Group, and one for Everyone.

To delete an entry, mouse over the entry and select the trash can icon.

To edit an entry, mouse over the entry and select the pencil editing icon.

To add an entry, click the **+ icon**.

After making changes, click the **APPLY** button.

Because this is a group share, full access may be granted to the group. To modify the **Root Directory ACL** for the group:

- Mouse over the ACL entry and select the pencil editing icon.
- To set the ACL entry to full control, on the Edit ACL Entry page, select **Full Control** from the dropdown box at the top of the page as shown in Figure 24.
- Click the **OK** button.

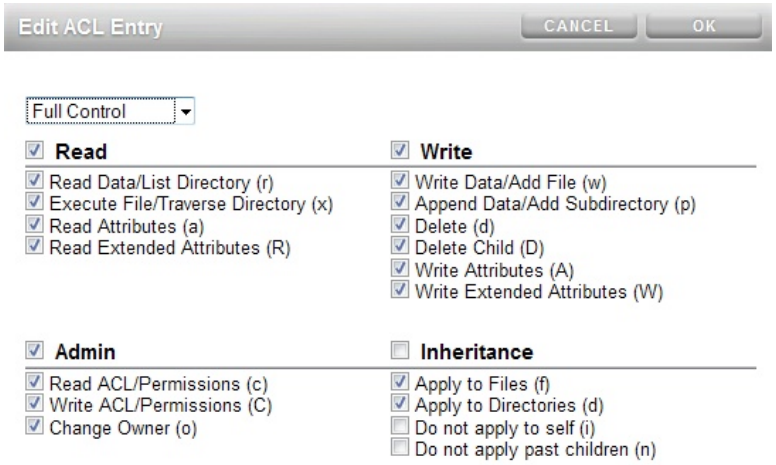

Figure 23: Editing the root directory ACL for group

Examples of Mapped Users and Groups

User Mappings

Figure 25 and Figure 26 demonstrate seamless access to the same share via SMB and NFS by two users: *ad-user* and *nis-user*. These two users were mapped to each other in the section Adding Rule-Based Mappings for an Individual User or Group.

In this example, the *ad-nis-user* share exists on the Sun ZFS Storage Appliance and has been mapped to or mounted by both the Windows client and the Solaris client. The user *ad-user* has created a directory called `Windows` and the user *nis-user* has created a directory called `Solaris` in the *ad-nis-user* share from a different platform. Figure 25 shows that the Security tab and Owner tab details are identical for both directories.

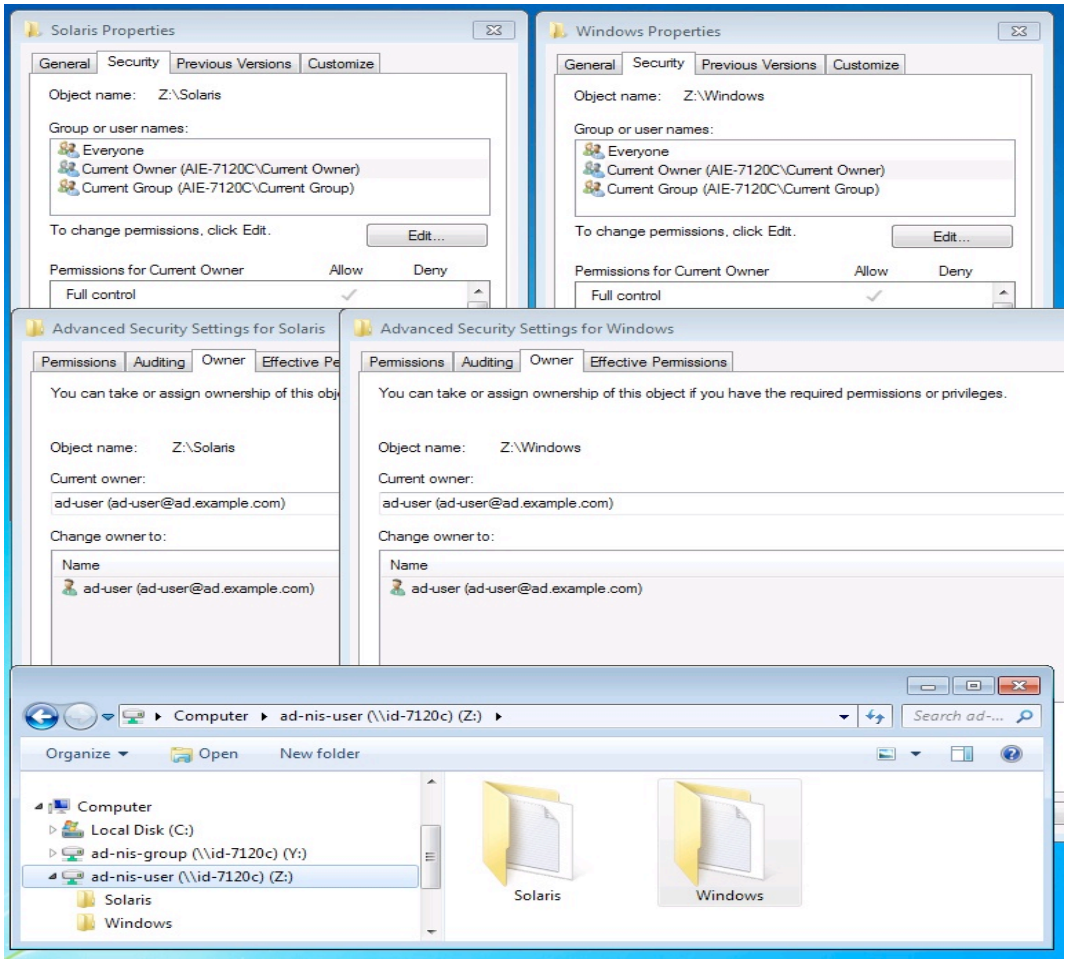

Figure 24: Windows mapped user example

Figure 26 displays the terminal output for the *ad-nis-user* directory on the Solaris client. This Solaris system belongs to the `nis.example.com` domain and the directory *ad-nis-user* has been mounted to the home directory of the user *nis-user* at `/home/nis-user`. Output from the `ls -lV` command displays the compact ACL output for this directory listing showing that both directories are identical and were created from two different platforms.

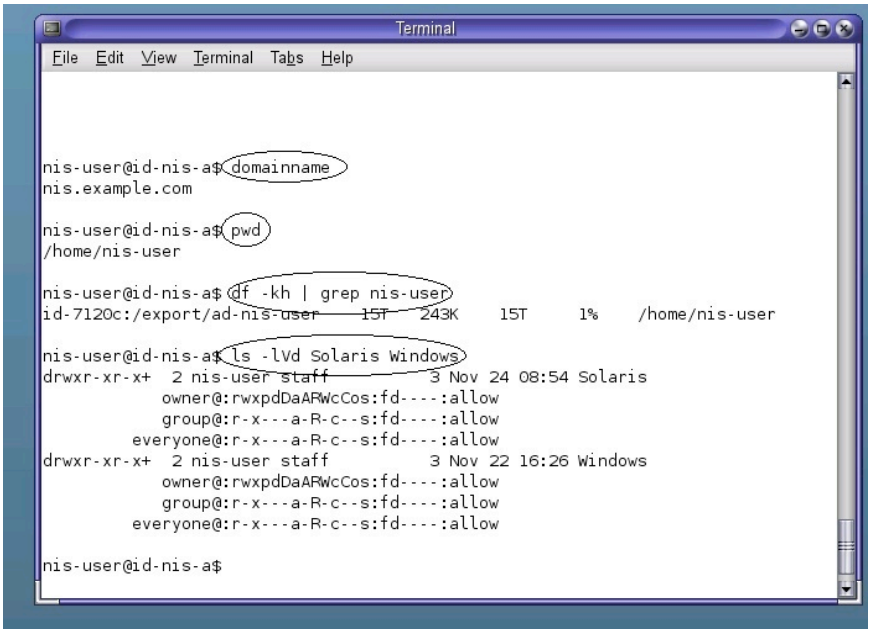

Figure 25: Solaris mapped user example

Group Mappings

Figure 27 and Figure 28 show seamless access to the same group share by the group *ad-group* on a Windows system and the group *nis-group* on a Solaris system. These two groups were mapped to each other in the section Adding Rule-Based Mappings for an Individual User or Group. In this case, Windows and Solaris directories have been created in a group share called *ad-nis-group* and mounted by the *ad-group* on a Windows system and the *nis-group* on a Solaris system. Figure 27 shows that full access (Full control) has been granted to the *ad-nis-group* group share for these groups (see the section Configuring Group Share-Level Access Settings*)*.

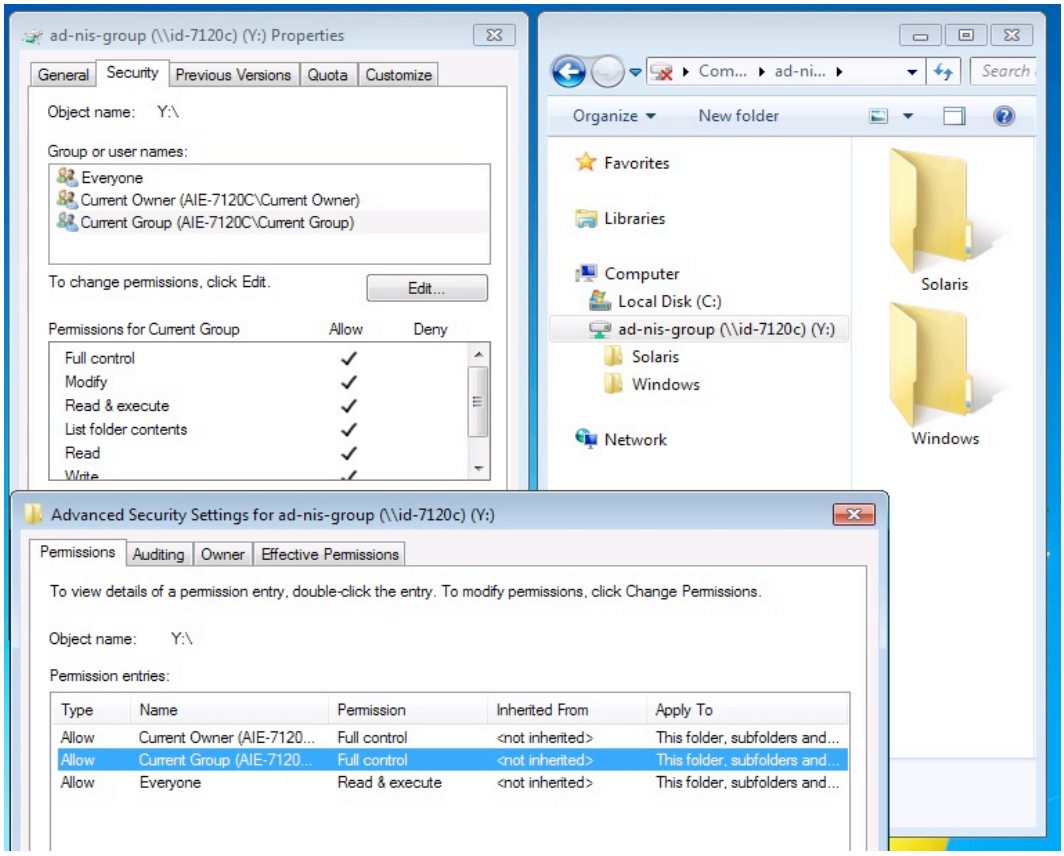

Figure 26: Windows mapped group example

Figure 28 displays terminal output for the *ad-nis-group* directory on the Solaris client. This Solaris system belongs to the `nis.example.com` domain and the user *nis-user* belongs to the group *nis-users*. The directory `ad-nis-group` has been mounted to `/mnt/ad-nis-group` from the Sun ZFS Storage Appliance on the client system.

Output from the `ls -lV .` command displays the compact ACL output for the `ad-nis-group` directory showing that the owner is *ad-nis-group*: `root` and *nis-group* is the group with full control. Output from the `ls -lV` command shows the compact ACL output for the two directories created in the `ad-nis-group` directory by the Windows and Solaris clients showing again that both directories are identical and the mapping is seamless.

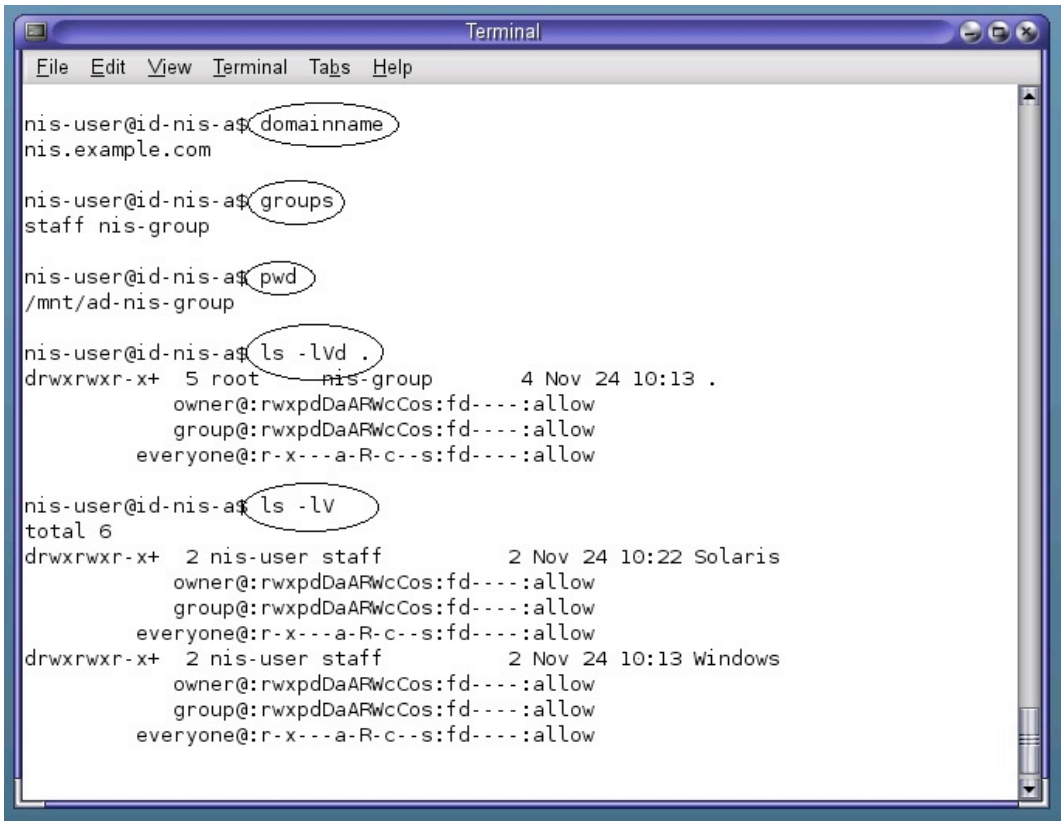

Figure 27: Solaris mapped group example

Quick Troubleshooting Q&A

Q: I cannot join my appliance to the Active Directory domain.

A1: Verify the appliance DNS settings are correct and check that a DNS record exists for the appliance in DNS.

A2: Make sure the user who is performing the join to the Active Directory domain has domain admin rights.

A3: Check that the appliance clock is in sync with the domain controller clock.

A4: Verify that the LAN Manager Compatibility Level settings described in the section Troubleshooting SMB Services are correct.

A5: Use the IP address of the server specified for the NIS domain on the NIS Services page (see Joining the Appliance to the NIS Domain*)*

A6: If jumbo frames are used on the appliance to be joined to the Active Directory, they need to be used on the Active Directory server as well.

Q: My SMB service is green, but I cannot see my shares from a client.

A: Make sure the SMB resource name for the file system is not set to **off** at either the project or share-level. See the section Configuring and Assigning Shares.

Q: I don't see an NFS share on my Solaris client, or I see an NFS share that has been removed from the appliance.

A1: It may take some time for the Solaris `automounter` or `autofs` services to update.

A2: Check that the NFSv4 identity domain of the client and the server are the same.

Conclusion

Rule-based identity mapping on the Sun ZFS Storage Appliance provides a simple, quick way to map user and group identities between Windows Active Directory and Solaris NIS directory services. Once the initial setup of the Sun ZFS Storage Appliance has been completed and the Windows and NIS domains populated with users and groups, domain-wide mapping rules can be created with wild cards or on a user-by-user or group-by-group basis using the appliance interface.

Reference Material

- Sun Unified Storage
- Solaris SMB/CIFS Service Troubleshooting
- Alan Wright's SMB/CIFS Solaris Blog
- Sun ZFS Storage Appliance Software
- Unified Storage For Dummies, Oracle Special Edition
- ZFS Storage Appliance Resource Kit
- Oracle's Sun Unified Storage Simulator

Sun ZFS Storage Appliance Rule-based Identity Mapping Between Active Directory and NIS Implementation Guide
February 2011, Version 1.1
Author: Art Larkin

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together