ETERNUS DX/AF Authentication Using Active Directory

Ability to manage administrative user IDs for various IT equipment like Storage Arrays have gained increased importance in the recent years. Having the user IDs managed by central directory systems such as Microsoft® Active Directory offers advantages for both the administrative users and the security management organization. An administrative user does not have to contend with having to remember multiple IDs and passwords for IT equipment and gain the convenience of the Single Sign On ability.

It offers advantages to the management side because the granting and revocation as well as monitoring of user accounts can be managed at a central location and discourages the all too common practice of assigning shared trivial passwords to various IT equipment. Even though IT equipment is typically located inside the firewall, we hear too often about the firewall being penetrated by sophisticated malware.

ETERNUS® DX/AF offers seamless integration with Active Directory through its RADIUS interface which is built-in as part of the Windows® Operating System as the Network Protocol Services role. Fine grained control of roles and privileges through the ETERNUS RBAC (Role Based Access Control) feature is fully supported through the Active Directory.

This paper documents the detailed procedure on how to implement Active Directory Integration for ETERNUS DX/AF management authentication.
Table of Contents

Overview of RADIUS/Active Directory Integration ................................................................................................................. 4
The procedure for setting up the RADIUS service on Windows Server 2012R2 and 2008R2 ................................................................................................................................. 6
(1) (Windows 2012R2) Install the Network Policy Services (NPS) Role ......................................................................................................................... 6
(2) (Windows 2008R2) Install the Network Policy and Access Services (NPS) Role ................................................................................................. 11
Set up ETERNUS DX/AF unit as a RADIUS Client ................................................................................................................................. 12
(3) Open the Network Policy Server (NPS) to define new RADIUS Client .................................................................................................... 12
(4) Fill in information regarding the ETERNUS DX/AF ................................................................................................................................. 12
(5) Set up the RADIUS client in the ETERNUS DX/AF GUI ............................................................................................................................... 13
Prepare Active Directory User accounts and Security Group Definitions .......................................................................................... 14
(6) Select Users being authorized for ETERNUS DX/AF Access ..................................................................................................................... 14
(7) Enable Reversible Password Encryption for the selected users ........................................................................................................... 15
(8) Ask the affected users to login and reset their passwords ....................................................................................................................... 15
(9) Configure the User Groups ............................................................................................................................................................ 15
Define Network Policy for each Role/Group Access ................................................................................................................................. 18
(10) Create new Network Policy ......................................................................................................................................................... 18
(11) Start the Network Policy wizard ....................................................................................................................................................... 18
(12) Continue the Network Policy Wizard: Specify Conditions .............................................................................................................. 18
(13) Continue the Network Policy Wizard: Specify Access Permission .................................................................................................. 20
(14) Continue the Network Policy Wizard: Configure Authentication Methods ........................................................................................ 21
(15) Continue the Network Policy Wizard: Configure Authentication Constraints .................................................................................. 22
(16) Continue the Network Policy Wizard: Configure Settings ............................................................................................................. 23
(17) Add Vendor Specific Attribute .................................................................................................................................................... 24
(18) Complete the Network Policy Wizard ........................................................................................................................................ 26
(19) Define the Network Policy for the rest of the Roles/Groups ......................................................................................................... 27
Testing the new Active Directory based User Authentication ............................................................................................................ 28
(20) Testing user Benjamin Braddock .................................................................................................................................................. 29
(21) Testing user Thuy Nguyen ............................................................................................................................................................ 29
(22) Testing user Samuel L. Jackson .................................................................................................................................................... 30
Troubleshooting ........................................................................................................................................................................... 31
(23) Case #1 – Forgetting to update the password with Reversible Encryption: ......................................................................................... 31
(24) Case #2 - The authentication or accounting record could not be written failure ............................................................................... 32

List of Figures

Figure 1: Overview of ETERNUS DX/AF Active Directory Integration ................................................................................................................. 4
Figure 2: Add Roles and Features Wizard ..................................................................................................................................................... 6
Figure 3: Add Roles and Features Wizard ..................................................................................................................................................... 7
Figure 4: Add Roles and Features Wizard ..................................................................................................................................................... 7
Figure 5: Add Roles and Features Wizard: Select features ......................................................................................................................... 8
Figure 6: Add Network Policy and Access services .............................................................................................................................................. 9
Figure 7: Select role services ........................................................................................................................................................................ 10
Figure 8: Confirm installation selections .................................................................................................................................................. 10
Figure 9: Add NPS Role ............................................................................................................................................................................. 11
Figure 10: Select Role Services ................................................................................................................................................................. 11
Figure 11: Setup new RADIUS Client ....................................................................................................................................................... 12
Figure 12: New RADIUS Client setup ..................................................................................................................................................... 13
Figure 13: Modify RADIUS screen ......................................................................................................................................................... 14
Figure 14: Select Users Identified for ETERNUS DX/AF Access .................................................................................................................. 14
Figure 15: Enable Reversible Password Encryption ........................................................................................................................................... 15
Figure 16: Adding new ETERNUS DX/AF Role .............................................................................................................................................. 16
Figure 17: Define New Security Group object ............................................................................................................................................. 16
Figure 18: List of ETERNUS DX/AF Users and Security Groups ........................................................................................................ 17
Figure 19: Assigning a User to a Security Group ........................................................................................................................................................ 17
Figure 20: Creating new Network Policy ......................................................................................................................................................... 18
Figure 21: Network Policy Wizard (First Panel) ............................................................................................................................................. 18
Figure 22: Network Policy Wizard - Assign User Group under Specify Conditions ......................................................................................... 19
Figure 23: Network Policy Wizard - Summary of Conditions ..................................................................................................................... 20
Figure 24: Network Policy Wizard - Access Granted ....................................................................................................................................... 21
Figure 25: Network Policy Wizard - Configure Authentication Methods ...................................................................................................... 22
Figure 26: Network Policy Wizard - Configure Constraints ...................................................................................................................... 23
Figure 27: Network Policy Wizard - Configure Settings ............................................................................................................................. 24
Figure 28: Network Policy Wizard - Add Vendor Specific Attribute ........................................................................................................... 25
Figure 29: Network Policy Wizard - Specifying Vendor-Specific Attribute Information ........................................................................................................ 25
Figure 30: Network Policy Wizard - Configure VSA .......................................................................................................................................... 26
Figure 31: Network Policy Wizard - Summary page and completion .............................................................................................................. 27
Figure 32: Network Policy Summary Screen after defining all four policies ............................................................................................ 28
Figure 33: Logging in bbraddock with Domain ID .............................................................................................................................................. 29
Figure 34: Verifying login with engcloud\bbraddock .............................................................................................................................................. 29
Figure 35: Logging in tnguyen without domain id ............................................................................................................................................... 30
Figure 36: Verifying login with tnguyen .............................................................................................................................................................. 30
Figure 37: NPS Role Summary Page ................................................................................................................................................................. 31

List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Vendor Specific Attributes (VSA)</td>
<td>4</td>
</tr>
<tr>
<td>Table 2</td>
<td>ETERNUS DX/AF Built in Roles</td>
<td>15</td>
</tr>
<tr>
<td>Table 3</td>
<td>Table of new Network Policies created</td>
<td>27</td>
</tr>
<tr>
<td>Table 4</td>
<td>Table of ETERNUS DX/AF Authorized Users and Roles</td>
<td>28</td>
</tr>
</tbody>
</table>
Overview of RADIUS/Active Directory Integration

This document describes how to authenticate the users for ETERNUS DX/AF management interface access using Microsoft Active Directory by using the ETERNUS DX/AF built-in RADIUS Authentication.

The following diagram shows the overview of ETERNUS DX/AF Active Directory Integration which consists of the following four steps:

- Install the Network Policy and Access Services (NPS) role to your Active Directory Server
- Register the ETERNUS DX/AF unit as a RADIUS client in NPS and register the Active Directory server to ETERNUS DX/AF.
- Identify the ETERNUS DX/AF authorized users, enable reversible password encryption and refresh their passwords.
- Define Network Policy and Security Groups for each Role being used and register.

![Diagram of ETERNUS DX/AF Active Directory Integration]

**Figure 1: Overview of ETERNUS DX/AF Active Directory Integration**

- RADIUS Authentication can be used to authenticate ETERNUS DX/AF access for both ETERNUS Web GUI and ETERNUS CLI.
- Up to two RADIUS servers (Active Directory Servers) can be connected to an ETERNUS DX/AF.
  - If the primary server times out, the secondary server is accessed for authentication.
- To use RADIUS Authentication with Active Directory, the User groups corresponding to each ETERNUS DX/AF Role must be pre-registered.
- Each new User Group defined for ETERNUS DX/AF access is assigned a following Vendor Specific Attribute which is a string with the name of the ETERNUS Role:

<table>
<thead>
<tr>
<th>Item</th>
<th>Size (octets)</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>1</td>
<td>26</td>
<td>Attribute number for the Vendor Specific Attribute</td>
</tr>
<tr>
<td>Length</td>
<td>1</td>
<td>7 or more</td>
<td>Attribute size (calculated by the server)</td>
</tr>
<tr>
<td>Vendor-Id</td>
<td>4</td>
<td>211</td>
<td>Fujitsu Limited (SMI Private Enterprise Code)</td>
</tr>
<tr>
<td>Vendor type</td>
<td>1</td>
<td>1</td>
<td>ETERNUS-Auth-Role</td>
</tr>
<tr>
<td>Vendor length</td>
<td>1</td>
<td>2 or more</td>
<td>Attribute size described after the Vendor type (calculated by the server)</td>
</tr>
<tr>
<td>Attribute-Specifier</td>
<td>1 or more</td>
<td>ASCII characters</td>
<td>List of one or more role names assignable to successfully authenticated users</td>
</tr>
</tbody>
</table>

1 The server-side role names are case sensitive and must be set correctly to match the ETERNUS defined Roles. (e.g. Admin, Maintainer Software etc.)
There are two types of authentication method supported by ETERNUS DX/AF RADIUS Client: CHAP and PAP. CHAP is the preferred method due to more robust security. This example assumes that CHAP is being used.

The use of CHAP authentication necessitates that the User’s password stored using “Reversible Password Encryption”. First, the “Reversible Password Encryption” must be enabled for the authorized users and then the user password must be updated in order for the password with Reversible Encryption to be stored.  

If RADIUS Authentication fails and “Do not use Internal Authentication” has been selected for “Authentication Error Recovery”, it will not be possible to login to ETERNUS Web GUI or ETERNUS CLI.

When 'Use Internal Authentication (Network Error Case)” has been selected for “Authentication Error Recovery”, Internal Authentication is only performed if RADIUS Authentication fails on both primary and secondary RADIUS servers, and at least one of these failures is due to network error.

So long as there is no RADIUS Authentication response the ETERNUS DX/AF will keep retrying to authenticate the user for the entire “Timeout” period set on the “Set RADIUS Authentication (Initial)” menu. Authentication not succeeding before the timeout occurs is considered a RADIUS Authentication failure.

When using RADIUS Authentication, if the role that is received from the server is unknown (not set) for the storage system, RADIUS Authentication fails.

---

2 There is a security implication of enabling Reversible Password Encryption. A stored encrypted password can be decrypted by knowledgeable users. Please read the following Microsoft TechNet Article [https://technet.microsoft.com/en-us/library/hh994559](https://technet.microsoft.com/en-us/library/hh994559) to understand the security implication. We recommend that the use of Reversible Password Encryption limited to the user accounts which need to access ETERNUS DX/AF using this method.
The procedure for setting up the RADIUS service on Windows Server® 2012R2 and 2008R2

The procedure for setting up the RADIUS service using Active Directory Instance on Windows Server 2008 R2 and Windows Server 2012R2 is outlined here. The GUI interface for the Windows 2012R2 and 2008R2 for Adding Roles is different but the subsequent steps are identical.

(1) **(Windows 2012R2) Install the Network Policy Services (NPS) Role.**

Steps (1) and (2) describe adding the NPS role. Step (1) describes the sequence on Windows 2012R2 and Step (2) describes the same sequence on Windows 2008R2:

Open Add Roles and Features Wizard on Windows 2012R2 as shown below:

![Add Roles and Features Wizard](image)

Figure 2: Add Roles and Features Wizard

Clicking on the NPS Role checkbox will pop up a confirmation dialog to add the required Features. Click "Add Features" to confirm.

---

3 It must be noted that this setup procedure is not necessarily guaranteed to work for all network and Active Directory environments. Make sure to obtain your system administrator's help in setting up the system.
Go back to the Add Roles and Features Wizard with the Check Mark enabled for NPS. Continue to Next step.

Next step is to select Features. The required features are pre-selected. Continue to Next step.
Next step shows some notes. The only option we are interested in is for NPS to act as the RADIUS server and proxy.
Figure 6: Add Network Policy and Access services

Select the role services screen, just keep the Network Policy Server (Default) and hit Next.
Confirm installation selections and hit the Install button:

![Figure 8: Confirm installation selections](image)
This completes the addition of NPS role on Windows2012R2, please proceed to Step 3.

(2) (Windows 2008R2) Install the Network Policy and Access Services (NPS) Role
Use the “Add Roles Wizard” and select “Network Policy and Access Services” to the Active Directory Server as shown in Error! Reference source not found.

![Figure 9: Add NPS Role](image)

Continue the Wizard selecting only the base Network Policy Server with no additions (default) as shown below:

![Figure 10: Select Role Services](image)
Setup ETERNUS DX/AF unit as a RADIUS Client

(3) Open the Network Policy Server (NPS) to define new RADIUS Client
Right Click on RADIUS Client menu item and select ‘New’ as shown below in Figure 11: Setup new RADIUS Client:

![Image of Network Policy Server](image)

Figure 11: Setup new RADIUS Client

(4) Fill in information regarding the ETERNUS DX/AF
On the new RADIUS Client, fill in the information regarding the ETERNUS DX/AF Storage array.
- Enable Check on “Enable this RADIUS client
- Enter Friendly name: (e.g. DX200S3-3)
- Enter the IP address of the ETERNUS management interface (e.g. 129.212.106.238)
- Setup Shared Secret: You can either enter some fixed phrase or choose to generate a 64 byte random shared secret. In this example the Generate option is used to generate a random string. 4
- Copy the generatedShared Secret to a Clipboard to be used to setup in the ETERNUS DX/AF side.

Once all the fields in the Setting panel are complete, hit the OK button and close.
There is no need to touch the contents under the “Advanced” tab.

---

4 The generated shared secret by MS Windows is 64 characters long. The ETERNUS DX S2 generation as well as the DX S3/S4 and AF series do support 64 byte shared secret. However, the prior generations (ETERNUS DX80/DX90/DX440 etc.) do not. If you are using the older ETERNUS units please truncate the generated key to less than or equal to 32 characters.
(5) Set up the RADIUS client in the ETERNUS DX/AF GUI

Login to the ETERNUS GUI and go to System -> User Settings -> Modify RADIUS Settings to configure the ETERNUS DX/AF RADIUS client.

Fill in the following information in the panel:

- **RADIUS Authentication** – Enable
- **Recovery Mode** – Yes (Communication Error/Authentication Error)
  
  Note: In this mode the accounts defined locally in the ETERNUS DX/AF unit such as "root" are still usable. Use this mode for now, once the authentication using Active Directory has been well established you can switch to a stricter mode to prevent back door access.

- **Primary Server**
  - Domain Name/IP Address: The IP address of the Active Directory and NPS Server (e.g. 129.212.106.254)
  - Port No: 1812 (Leave it at default)
  - LAN Port: MNT (Leave it at default)
  - Authentication mode – CHAP
  - Shared Secret: Paste the generated Secret key from the Active Directory Server
  - Retry Out Time: 30 sec (Leave it at default)

- The Secondary Server is not being configured in this example.

Once all the fields are filled in hit the ‘Modify’ button to complete this step.
Prepare Active Directory User accounts and Security Group Definitions.

It is necessary for the accounts using the CHAP authentication to use the “Reversible Password Encryption.” This can be done by identifying the users, which require access to ETERNUS DX/AF and then enable “Reversible Password Encryption” to all of these users. It is necessary for the users to reset the password afterwards so that the password with reversible encryption is stored.

(6) Select Users being authorized for ETERNUS DX/AF Access.
For example, assume you have identified four users in your organization to have access to the ETERNUS DX/AF with various roles. Select all the candidate users as shown below in Figure 14: Select Users Identified for ETERNUS DX/AF Access:
Enable Reversible Password Encryption for the selected users. With the Users selected open Properties: Enable check marks on "User must change password at next logon" and "Store Password using Reversible Encryption" as shown below in Figure 15: Enable Reversible Password Encryption.

![Figure 15: Enable Reversible Password Encryption](image)

Ask the affected users to login and reset their passwords. This step is important; the Login to ETERNUS DX/AF will fail unless the password is updated with Reversible Encryption so it is important that the users refresh the password after the reversible encryption is enabled.

Configure the User Groups
An Active Directory User Group must be created for each ETERNUS DX/AF role that you intend to use:
The role may be one of the seven built-in roles shown in Table 2, or it can be custom built:

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor</td>
<td>Allow monitoring only, no configuration changes.</td>
</tr>
<tr>
<td>Admin</td>
<td>All Administrator functions including User accounts.</td>
</tr>
<tr>
<td>StorageAdmin</td>
<td>All Storage Provisioning functions</td>
</tr>
<tr>
<td>AccountAdmin</td>
<td>User account management</td>
</tr>
<tr>
<td>SecurityAdmin</td>
<td>Security auditing functions</td>
</tr>
<tr>
<td>Maintainer</td>
<td>Hardware and Firmware Maintenance Functions</td>
</tr>
<tr>
<td>Software</td>
<td>CLI Only Used only for Software API interface (e.g. ESF, PMCC etc.)</td>
</tr>
</tbody>
</table>

In this example, we will use three built-in roles:
- Admin
- Maintainer
- Software

Additionally we will create one Custom role.

Custom role is created using the ETERNUS GUI:
Login to ETERNUS DX/AF using the root (or admin role) account and then go to: System -> User Settings -> Add Role

In this example, we will create a new role called "superadmin" with Policies defined as shown below:
For each role intended for use at your organization, it is necessary to create a new Security Group Object using the Active Directory Users and Computers tool. The Group name does not have to match the role name but it would be a good idea to include the role name as part of the Group name for mnemonic purposes. In this example we will create the four groups by adding a “DX_” prefix to the role name. (i.e. DX_Admin, DX_Maintainer, DX_Software, DX_superadmin).
Once all the groups are created the list of Users and Groups looks like the below example:

![List of ETERNUS DX/AF Users and Security Groups](image1)

Now we should assign each user to one of the Security groups.

In this example, we will use the following assignment:

- Benjamin Braddock -> DX_Admin
- Elaine Robinson -> DX_Maintainer
- Samuel L. Jackson -> DX_Software
- Thuy Nguyen -> DX_superadmin

The Figure below shows an example of adding Elaine Robinson to the DX_Maintainer Group:

![Assigning a User to a Security Group](image2)
Define Network Policy for each Role/Group Access

For each new Security Group created in the previous step we need to define a new Network Policy. Network Policy ties the Security Group, Role Name and Authentication Methods to define how the Login by ETERNUS RADIUS Client is authenticated.

(10) Create new Network Policy

Open the NPS tool and select NPS(local)->Policies->Network Policies and Right Click and select "New" as shown below:

![Figure 20: Creating new Network Policy](image)

(11) Start the Network Policy wizard

The network policy wizard starts with the Policy name. In this example we will use the same Policy name to match the Security Group name previously defined. (i.e. Policy name -> Security Group Name, DX_admin -> DX_admin, DX_maintainer -> DX_maintainer)

![Figure 21: Network Policy Wizard (First Panel)](image)

(12) Continue the Network Policy Wizard: Specify Conditions

Next step in the Network Policy Wizard asks you to Specify Conditions, here we tie the Network Policy to the Security Group Name by assigning
the condition as "User Groups" and then select the corresponding Security Group name. In this case we are doing DX_Admin policy so we select the DX_Admin user group:

![Network Policy Wizard - Assign User Group under Specify Conditions.](image)

**Figure 22: Network Policy Wizard - Assign User Group under Specify Conditions.**

The following screen shows how the conditions are defined after specifying the User Group.
(13) **Continue the Network Policy Wizard: Specify Access Permission**
Continuing the Network Policy Wizard, it asks to specify "Access granted" or "Access denied". Since we want to grant access to a user in group DX_admin we specify "Access granted" (Default):
Figure 24: Network Policy Wizard - Access Granted

(14) Continue the Network Policy Wizard: Configure Authentication Methods
Next screen in the Wizard asks for the Authentication Methods:
IMPORTANT: Checkbox for “Encrypted Authentication Method (CHAP)” must be enabled here. It is not enabled by default.
Figure 25: Network Policy Wizard - Configure Authentication Methods

(15) Continue the Network Policy Wizard: Configure Authentication Constraints
No change required in this panel – continue to the next panel.
Figure 26: Network Policy Wizard - Configure Constraints

(16) Continue the Network Policy Wizard: Configure Settings

We add the VSA (Vendor Specific Attributes) in this panel. Select “Vendor Specific” under RADIUS Attributes in the Settings menu and then hit the “Add” button to define new VSA:
Figure 27: Network Policy Wizard - Configure Settings

(17) Add Vendor Specific Attribute

A new dialog will appear after pressing the "Add" button. Scroll all the way down on the Attributes box and select "Vendor-Specific" and hit the "Add" button:
After pressing the Add Button, the "Vendor-Specific Attribute Information" dialog opens. The following information must be filled out:

- Specify network access server vendor: **Enter Vendor Code 211**
- Specify whether the attribute conforms to the RADIUS RFC specifications for vendor specific attributes: **Yes. It conforms**

Then press the "Configure Attribute" button to fill in further details.

On the Configure VSA (RFC Compliant) dialog, enter the following information:
Vendor-assigned attribute number: 1

- Attribute format: String
- Attribute Value: This is the name of the Role defined in ETERNUS DX/AF. This string is Case Sensitive. In this example it should be "Admin".

![Vendor-specific Attribute Information](image)

**Figure 30: Network Policy Wizard - Configure VSA**

(18) Complete the Network Policy Wizard

After completing the VSA the network Policy Wizard is finally complete. Review the summary screen to ensure that the information is filled out correctly and then press the "Finish" button. The summary information should be as follows:

- Policy Conditions: There should be one condition with "User Groups" and the User Group Name that corresponds to the Network Policy Name (i.e. DX_admin)
- Policy Settings - Verify the following settings
  - Authentication Method: **Encryption Authentication (CHAP)**...
  - Access Permission: **Grant Access**
  - Vendor-Specific: **Admin** (ETERNUS DX/AF defined Role name)
(19) Define the Network Policy for the rest of the Roles/Groups.

The bad news is that we need to define three more Network Policies. In this example we set out to define a total of four Network Policies as listed below.

In order to save time, you can duplicate the policy you just created and then modify the User Group and VSA according to the table.

Table 3: Table of new Network Policies created

<table>
<thead>
<tr>
<th>Network Policy</th>
<th>Security (User) Group</th>
<th>Role and VSA</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DX_Admin</td>
<td>DX_Admin</td>
<td>Admin</td>
<td>Administrator Role (Built in, same as root)</td>
</tr>
<tr>
<td>DX_Maintainer</td>
<td>DX_Maintainer</td>
<td>Maintainer</td>
<td>Maintenance Role (Built-in, same as f.ce)</td>
</tr>
<tr>
<td>DX_Software</td>
<td>DX_Software</td>
<td>Software</td>
<td>Software Role (Built-in, CLI only to be used by )</td>
</tr>
<tr>
<td>DX_superadmin</td>
<td>DX_superadmin</td>
<td>superadmin</td>
<td>Super Admin (Custom role created in this example)</td>
</tr>
</tbody>
</table>

After defining the rest of the Network Policies the summary page should look like the following:
This completes the NPS setup in Active Directory. Now we are ready to test the Authentication.

**Testing the new Active Directory based User Authentication.**

We are now ready to test the Authentication.

In this example we have made four Active Directory User IDs assigned to the four newly created Security Groups as summarized in the table below:

**Table 4: Table of ETERNUS DX/AF Authorized Users and Roles.**

<table>
<thead>
<tr>
<th>User Name</th>
<th>User ID</th>
<th>Security Group</th>
<th>Network Policy</th>
<th>Role and VSA</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benjamin Braddock</td>
<td>bbraddock</td>
<td>DX_Admin</td>
<td>DX_Admin</td>
<td>Admin</td>
<td>Administrator Role (Built in, same as root)</td>
</tr>
<tr>
<td>Elaine Robinson</td>
<td>eroberlin</td>
<td>DX_Maintainer</td>
<td>DX_Maintainer</td>
<td>Maintainer</td>
<td>Maintenance Role (Built-in, same as fcre)</td>
</tr>
<tr>
<td>Samuel L. Jackson</td>
<td>sjackson</td>
<td>DX_Software</td>
<td>DX_Software</td>
<td>Software</td>
<td>Software Role (Built-in, CLI only for Software API)</td>
</tr>
<tr>
<td>Thuy Nguyen</td>
<td>tnguyen</td>
<td>DX_superadmin</td>
<td>DX_superadmin</td>
<td>superadmin</td>
<td>Super Admin (Custom Role)</td>
</tr>
</tbody>
</table>
(20) Testing user Benjamin Braddock
Test access for the user Benjamin Braddock whose Id is "bbraddock". In this test we will specify the Domain name which is "engcloud".

Verify successful login:
After login go to "System" tab to verify the login ID (engcloud\bbraddock) and Role (Admin).

(21) Testing user Thuy Nguyen
This time we test the user "tnguyen" who belongs to the User Group with Custom Role "superadmin". In this case we will not specify the Domain name5.

---

5 In this environment where the RADIUS server is connected to the Active Directory Server with single domain there is no need to specify the Domain Name in Login. This may differ depending on how the domain controller is configured.
Verify successful login:
After login go to the "System" tab to verify the login ID (tnguyen) and Role (superadmin).

Testing user Samuel L. Jackson
We can test the user "sjackson" who belongs to the User Group DX_Software.
The software role is specifically created for API access by software such as ESF and PMCC. It only supports CLI which uses a special interface. Just for validation purposes we can access the CLI with a SSH client as shown below:

```
Bash> ssh sjackson@129.212.106.238
FUJITSU Storage ETERNUS login is required. [2017-07-02 23:49:09]
Password:

CLI> show status
00
20 00
CLI> exit
Connection to 129.212.106.238 closed by remote host.
Connection to 129.212.106.238 closed.
```
Troubleshooting

Active Directory is a complex system and it is beyond our scope to help in case there are configuration issues with Active Directory. It is best to get appropriate help from those who have Active Directory expertise. However, here are some pitfalls you may run into when configuring the system.

The best place to check when the authentication does not work as intended is the Summary page of the Network Policy and Access Services (NPS) role. The summary page contains the Event logs associated with NPS:

![Figure 37: NPS Role Summary Page](image)

(23) Case #1 – Forgetting to update the password with Reversible Encryption:

Forgetting to update the password after enabling Reversible Encryption will result in the following “Audit Failure” Event:

<table>
<thead>
<tr>
<th>Log Name:</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source:</td>
<td>Microsoft-Windows-Security-Auditing</td>
</tr>
<tr>
<td>Date:</td>
<td>7/3/2017 12:21:51 AM</td>
</tr>
<tr>
<td>Event ID:</td>
<td>6273</td>
</tr>
<tr>
<td>Task Category:</td>
<td>Network Policy Server</td>
</tr>
<tr>
<td>Level:</td>
<td>Information</td>
</tr>
<tr>
<td>Keywords:</td>
<td>Audit Failure</td>
</tr>
<tr>
<td>User:</td>
<td>N/A</td>
</tr>
<tr>
<td>Computer:</td>
<td>CLOUDDC.engcloud.local</td>
</tr>
</tbody>
</table>

**Description:**
Network Policy Server denied access to a user.

Contact the Network Policy Server administrator for more information.

**User:**
- Security ID: NULL SID
- Account Name: bbraddock
- Account Domain: ENGCLOUD
- Fully Qualified Account Name: ENGCLOUD\bbraddock

**Client Machine:**
- Security ID: NULL SID
- Account Name: -
- Fully Qualified Account Name: -
- OS-Version: -
- Called Station Identifier: -
- Calling Station Identifier: -

**NAS:**
- NAS IPv4 Address: 129.212.106.238
- NAS IPv6 Address: -
- NAS Identifier: storage
- NAS Port-Type: -
- NAS Port: -

**RADIUS Client:**
Case #2 - The authentication or accounting record could not be written failure

The following failure occurred in our case because the storage in the Active Directory server was exhausted. This error may also occur if the Network Access Protection - > Accounting information for where the logs are saved are incorrectly specified.

---

Log Name: Security
Source: Microsoft-Windows-Security-Auditing
Date: 6/28/2017 5:38:28 PM
Event ID: 6274
Task Category: Network Policy Server
Level: Information
Keywords: Audit Failure
User: N/A
Computer: CLOUDDC.engcloud.local
Description: Network Policy Server discarded the request for a user.

Contact the Network Policy Server administrator for more information.

User:
- Security ID: ENGCLOUD\kkatsumata
- Account Name: Engcloud\kkatsumata
- Account Domain: ENGCLOUD
- Fully Qualified Account Name: engcloud.local/Users/Kun Katsumata

Client Machine:
- Security ID: NULL SID
- Account Name: -
- Fully Qualified Account Name: -
- OS-Version: -
- Called Station Identifier: -
- Calling Station Identifier: -

NAS:
- NAS IPv4 Address: 129.212.106.238
- NAS IPv6 Address: -
- NAS Identifier: storage
- NAS Port-Type: -
- NAS Port: -

RADIUS Client:
- Client Friendly Name: test
- Client IP Address: 129.212.106.238

Authentication Details:
- Connection Request Policy Name: Use Windows authentication for all users
- Network Policy Name: test-policy
- Authentication Provider: Windows
- Authentication Server: CLOUDDC.engcloud.local
- Authentication Type: MD5-CHAP
<table>
<thead>
<tr>
<th>EAP Type</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Session Identifier</td>
<td>-</td>
</tr>
<tr>
<td>Reason Code</td>
<td>80</td>
</tr>
<tr>
<td>Reason</td>
<td>The authentication or accounting record could not be written to the configured accounting datastore. Ensure that the log file location is accessible, has available space, can be written to and that the directory or SQL server is available.</td>
</tr>
</tbody>
</table>