How to enable Active Directory authentication in DASH Systems with Broadcom Management Controller

This document outlines the steps required to configure DASH systems based on Broadcom Management Controller for active directory authentication.

Requirements

1. Administrator access to the domain controller
2. Ensure Broadcom Manageability Configuration and Control (BMCC) command line tool is installed on the DASH System. Refer OEM documentation on obtaining this application. Alternatively, DASH Config utility can be used instead of BMCC. DASH Config application is packaged and is available at <install folder>/DASHConfig/.

Note: The steps are tested on Windows 2008 R2 domain controller.

Steps

1) Create SPN user

On the domain controller, using the command 'net user /domain /add <username> <password>', add DASH service principal user account. Example,

```
net user /domain /add DASHSpnUser DashSpnUser_Password
```

Note: It is recommended that this user account be of least privileges and protected by strong password. This account need not have desktop logon rights.

2) Register SPN user for HTTP service

On the domain controller, register the SPN user for HTTP service for the DASH system. If the DASH system's FQDN (fully qualified domain name) is DASHSystem.XYZ.Com, run the commands:

```
setspn -A http/DASHSystem.XYZ.Com DASHSpnUser
setspn -A http/DASHSystem DASHSpnUser
```

3) Obtain user account SID

On the domain controller, run the command,

```
wmic useraccount get name,sid
```

Output will be in the format,

```
 Name           SID
 Administrator  S-1-5-21-3672929279-565669401-094452374-500
...
```

Copy the SID value of the corresponding user account, which will be used for active directory authentication. In this example, Administrator account will be used for active directory authentication. Hence the SID will be 'S-1-5-21-3672929279-565669401-094452374-500'.

Note: If the SID of group is obtained, then all users of that group will be enabled for active directory authentication. SID of group can be got by the command,

```
wmic group get name,sid
```

4) Enable active directory authentication

On the DASH system, using bmcc command line tool, enable the active directory authentication. Sequence of commands is,

```
a) bmcc edit
b) Enter your choice -> w (for the label Web-based Management)
c) Enter your choice (item=value) -> 10 (for the label Active
   Directory Authentication)
   So that the setting is as,
   10. Active Directory Authentication....: Enabled
d) Enter your choice (item=value) -> 11=DashSpnUser_Password (for
   the label Active Directory Password)
e) Press Enter key and type q to save & exit.
```

Note: The password set in step (d) can be verified by the command,

```
   bmcc view –verbose -record=ad
```

5) Set SID of user account

On the DASH System, use bmcc command line tool to map SID of domain user to the role. Sequence of command are,

```
a) bmcc edit
b) Enter your choice -> u (for the label User Account Management)
c) Enter your choice -> 1 (for the label User Roles)
d) Enter your choice -> 1 (for the label Role - Administrator Role)
e) Enter your choice (item=value) -> 5=S-1-5-21-3672929279-
   565669401-094452374-500 (for the label Active Directory SID)
f) Press Enter key, again Enter key and type q to save & exit.
```

Note: Steps (4) & (5) can be performed with the packaged DASHConfig utility. Refer <install folder>/DASHConfig/ReleaseNotes.rtf for usage information.

Usage Example

DASH CLI commands can be used with active directory authentication, for instance such as:

```
dashcli -h dash-system -p 664 -S https -a gss -u DOMAIN\User -P
   userpass capabilities
```

If the logged in user is enabled for active directory authentication, then DASH CLI command can run in single sign on mode, such as:

```
dashcli -h dash-system -p 664 -S https -a gss capabilities
```

Note: For using self-signed certificates for HTTPS communication, refer the document 'DASHCertificates.pdf' in the 'docs' folder of DASH CLI installation.