Active Directory Authentication with DASH SCCM Plug-in

Document version: 1.1

Feb 12th, 2013

White Paper Descriptor

This whitepaper describes how to configure Active Directory authentication that can be adopted for performing desktop and mobile architecture for system hardware (DASH) operations on a DASH-capable system from Microsoft® System Center Configuration Manager 2007 using the DASH Plug-in.

Table of Contents

Introduction

Microsoft® System Center Configuration Manager 2007 R2 (SCCM) is the solution for comprehensively assessing, deploying, and updating servers, clients, and devices across physical, virtual, distributed, and mobile environments. Optimized for Windows desktop and Windows server platforms, it is widely considered the best choice for centralizing management from the data center to the desktop

The DASH Plug-in extends SCCM to support out-of-band management tasks using DASH. DASH Plug-in installs simply over SCCM and enables SCCM to perform out-of-band operations such as power/boot options, redirection etc., on a DASH-capable system.

Active Directory authentication offers users a faster, more secure, and more scalable authentication mechanism. By using the Kerberos authentication protocol, Secure Global Desktop (SGD) can authenticate any user securely against any domain in a forest. DASH Plug-in supports both Digest and Active Directory authentication. This document will cover how to use Active Directory authentication with DASH SCCM Plug-in.

Audience

This document is intended for IT administrators interested in using Active Directory authentication for DASH 1.0 and 1.1 capabilities such as discovery, remote power control, boot control, media redirection, text console/serial redirection etc. It provides a technical overview of how to use Active Directory Authentication with DASH SCCM Plug-in.

Prior Knowledge

The administrator using this guide should have prior knowledge of the following technologies:

- System Center Configuration Manager 2007
- Working knowledge of Active Directory settings in Windows Server 2003/2008
- DASH Plug-in for SCCM
- DASHConfig Tool

Pre-requisites

It is assumed that the following network/system, including authorization to access administrative consoles, is setup and ready to use.

- Administrative access to Domain Controller
- System with Microsoft® SCCM 2007 running on it
- DASH Plug-in for SCCM

Overview

For an IT Administrator to manage DASH systems effectively, a proper authorization setting needs to be implemented in both Active Directory domains as well as in the DASH targets. The administrator needs to set the service principal name (SPN) in the Active Directory so only authorized users can

communicate with the assigned DASH targets. The next section offers a brief description of how to create SPN account in groups, and users.

Create SPN account in Active Directory

Input the name of an account in the "Full name" and "User Logon name" edit fields. Record this account name for use in a later procedure.

Choose a password for this and record it. Follow your company's security policy while selecting and modifying the security settings for user credentials and passwords.

NOTE: For higher security, this user can have restricted access, such as no desktop logon access.

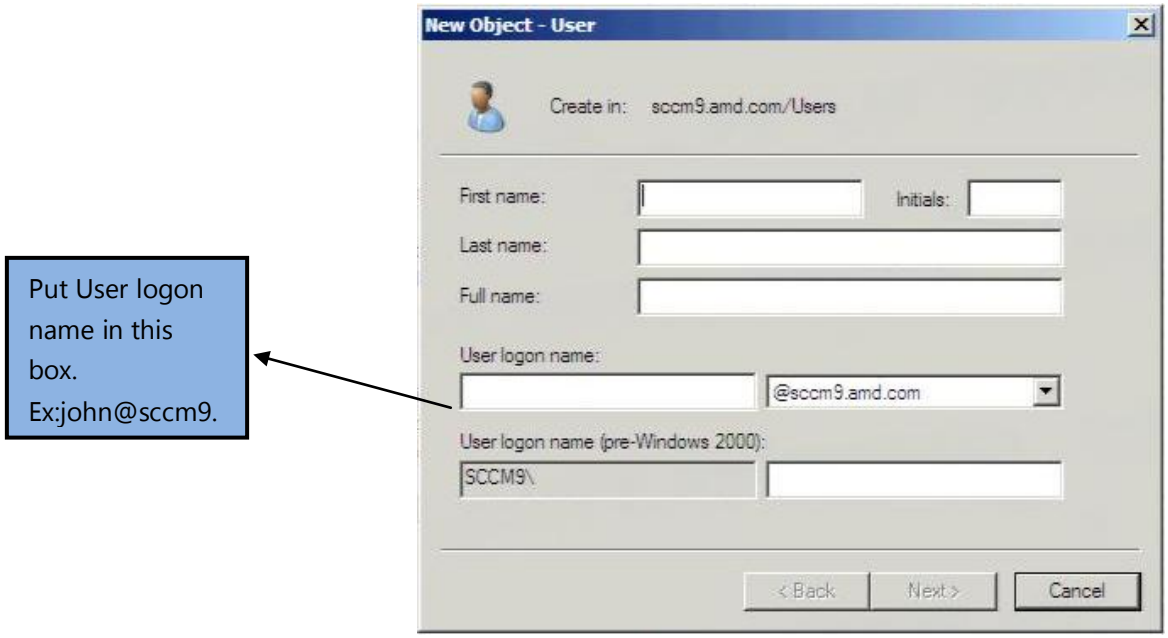

Figure 1: Create User

Register SPN for HTTP service on DASH system

Under the "Properties" for the user created in Figure 1, select the "Attribute Editor" tab. Add two values for each DASH system under the "servicePrincipalName" attribute item which is expected to use AD authentication. (see Figure 2)

The first value is in the form: HTTP/<MachineName>,
Example: HTTP/TGTONE
The second value is in the form: HTTP/<FQDN>,
Example: HTTP/tgtone.sccmtest.bigcorp.com

NOTE: For a large group of DASH systems, it is faster to use the SETSPN utility inside of script or batch file.

When using the SETSPN utility use the following two command line invocations:

Setspn –A HTTP/<MACHINENAME> <spnacctname>

Setspn –A HTTP/<FQDN> <spnacctname>

In our example, <MACHINENAME> is TGTONE, <FQDN> is tgtone.sccmtest.bigcorp.com and <spnacctname> is spnacctname

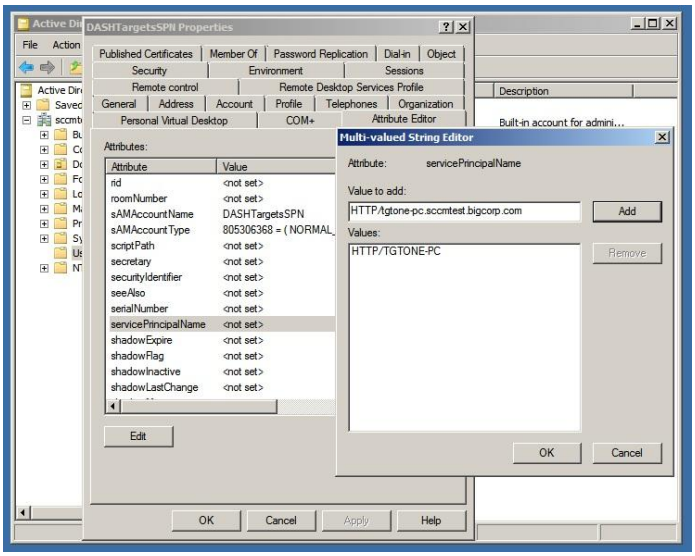

Figure 2: Set SPN

Create group in Active Directory and obtain SID

Create a security group

Enter a custom-defined group under the "Group Name" edit control. (Figure 3)

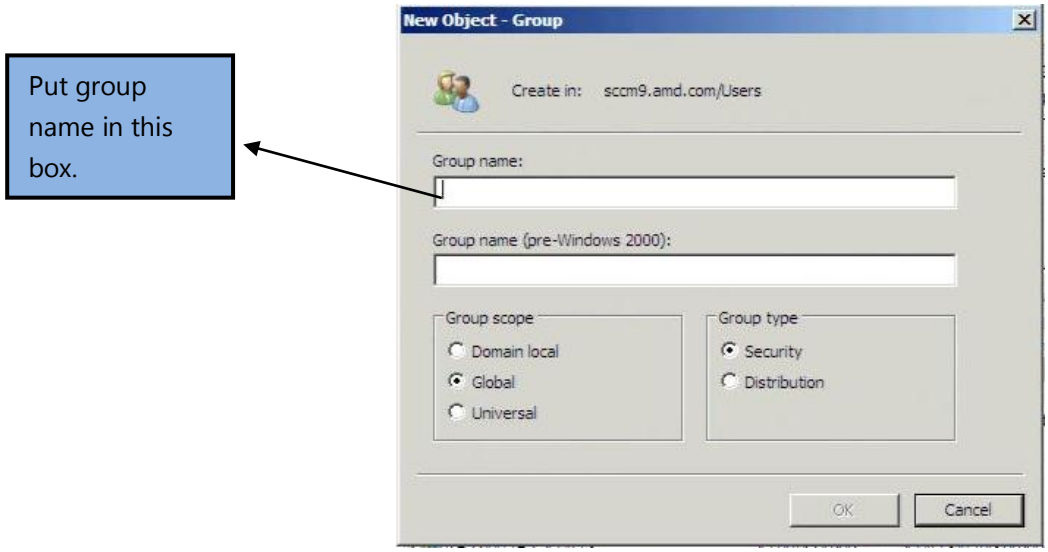

Figure 3: Create group

Obtain the security object ID for the LibrarySystems group

Under "Properties" menu for the group created in Figure 3, select "Attribute Editor" tab. Scroll down the "Attributes" list box until you find the "objectSID" attribute item. (Figure 4).

NOTE: Record the security ID string in the value field for the objectSID attribute. Depending on screen size, you may need to scroll to obtain the whole string. In this example, the security ID used was "S-1-5-21-372084433-2080421639-3642503678-1111".

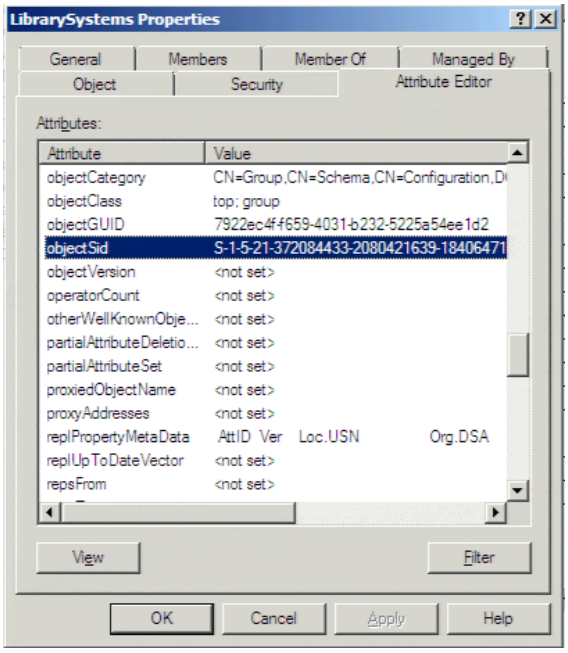

Figure 4: Obtaining SID value

Use DASHConfig to set SPN account and SID in DASH system

Update the DASHConfig provisioning XML file for distribution

Obtain the DASHConfigExample.xml file (this can also be found in Appendix B at the end of this paper) from the DASHConfig package and open it in the text editor of your choice.

Modify the following XML nodes with information from the previous procedures:

<ACTIVEDIRECTORY_SPNACCOUNT> The SPN account created in the procedure shown in Figure 1.
<SPNACCOUNT_PASSWORD> The password selected for the created user.<OBJECTSID> from the
<ACTIVEDIRECTORY_GROUP> The ADGroup created in procedure shown in Figure 3.

Save the changed file. In this example, it was saved as DASHConfigExample.xml

Run DASHConfig utility on DASH system

The DASHConfig utility can run on DASH systems manually or can be sent as package from SCCM. Both methods are described in this paper.

Add user to the created group

Under the "Properties" of the user created, open "Member Of" tab and add the created group to it as shown in Figure 5.

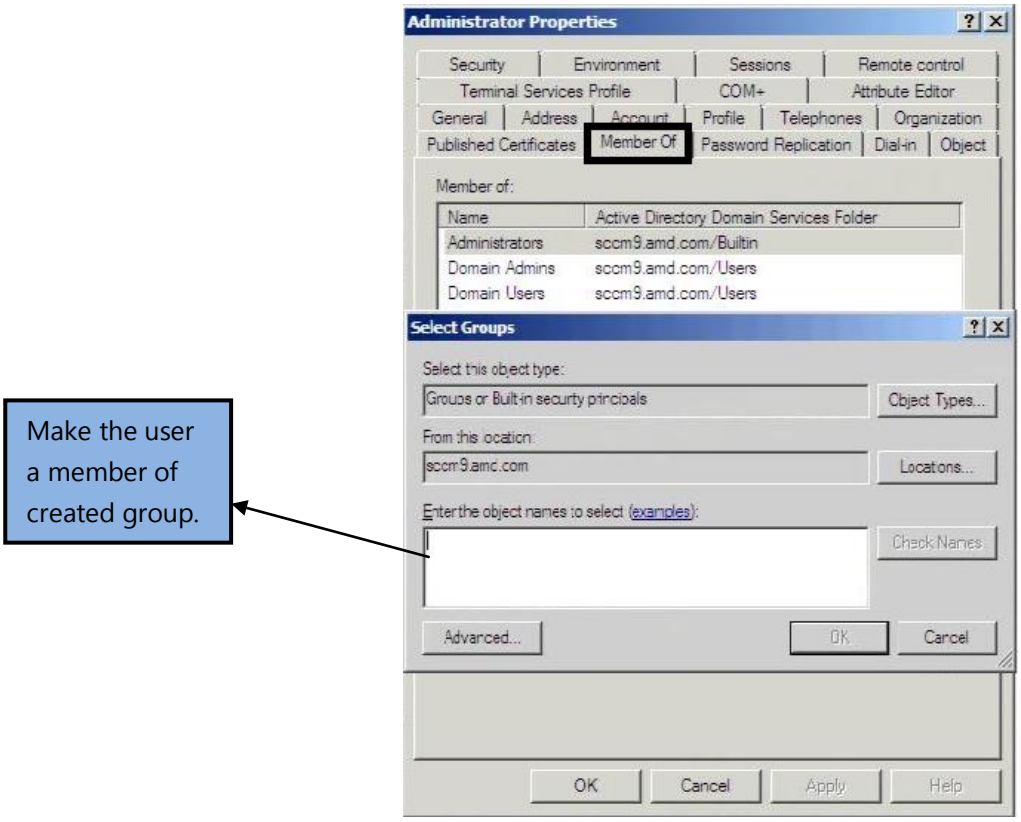

Figure 5: Adding user to the created group

Configure DASH Plug-in

a. Open DASH Management Properties in DASH Plug-in
b. Go to Authentication tab.
c. Check "Enable Active Directory Authentication" to enable Active Directory.
d. Enter the DASH systems user created earlier (Figure 1) as domain user and specify correct password for that account.
e. Check "Use Active Directory as Default Authentication" to select Active Directory as default.
f. Click OK when done.

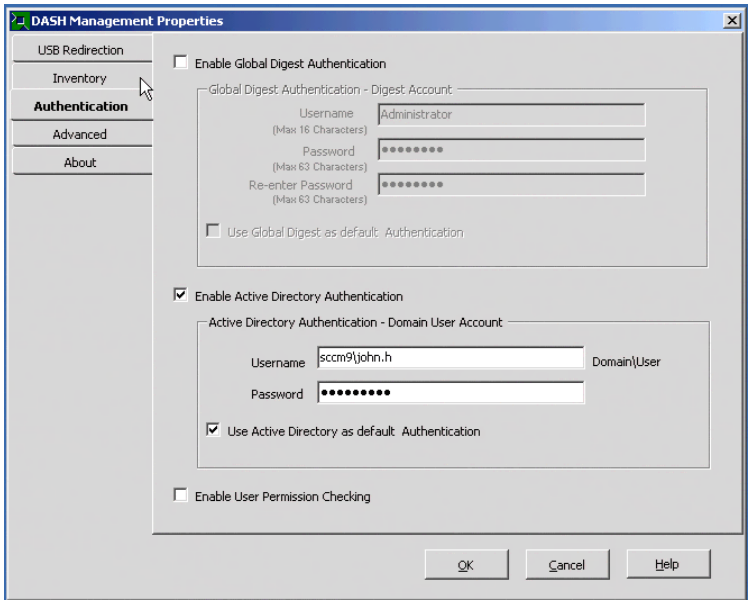

Figure 6: Authentication tab

Frequently Asked Questions

User Messages

Q: What is SPN in Active Directory?

A: A service principal name (or SPN), is the name by which a client uniquely identifies an instance of a service. If you install multiple instances of a service on computers throughout a forest, each instance must have its own SPN. A given service instance can have multiple SPNs if there are multiple names that clients might use for authentication.

Q: What is Object SID value and why it is required

A: A security identifier (commonly abbreviated SID) is a unique, immutable identifier of a user, user group, or other security principal. A security principal has a single SID for life, and all properties of the principal, including its name, are associated with the SID.

Glossary

The following terms are used to describe the components of Active Directory authentication and DASHConfig

DASH	Desktop Mobile Architecture for System Hardware, the new DMTF commercial client management standard produced by the DMTF DMWG. Specifies the transport, management protocol (WS-Man), and DMTF CIM profiles used to manage desktop/mobile PC. A "Dash capable system is a computer system that conforms to the DMTF DASH standard.
DASH capable systems	Machines with DASH-enabled NICs.
Out-of-band	Management tasks that are performed independent of the power or OS state on the managed client or system.
SCCM	Microsoft® System Center Configuration Manager 2007.
MMC	Microsoft Management Console
AD	Active Directory
DASHConfig	DASHConfig is a provisioning tool developed by AMD to configure DASH targets

Conclusion

Active Directory authentication with the DASHConfig utility provides greater security to administrators performing DASH operations.

Appendices

Appendix A - Case study

Educational Institute Scenario

In an Educational Institute, there are three different departments, Library, Arts and Science. They are in different geographical locations. Each of the three departments have about 500 DASH-compatible machines. The IT administrator defines three groups "LibrarySystems", "ScienceSystems" and "ArtsSystems". All users allowed to manage Library department systems are added to DASHLib group. A new member (john.h) is hired to manage the DASHLib systems.

Problem

The new hire should have ability to manage all the 500 systems. Adding new-hire login credentials to all the machines is cumbersome and time-consuming because the systems are located in geographically diverse locations.

Solution Description

The IT administrator adds (john.h) in the LibrarySystemsgroups. "john.h" logs in with his credentials and can manage the DASH systems for all 500 machines under the Library department, and he does not need to provision each system separately. This also allows user role-based access (RBA), in which the Library administrator may not have permission to perform DASH/remote execution operations on systems located in Science department.

Steps:

1. Create a SPN with unique username/password who has very limited privileges on an Active Directory domain.

2. Register the SPN for HTTP Service on all DASH systems under library group (Administrators can use batch scripting to register all 500 systems)

3. Obtain object SID value for the "LibrarySystems" group and assign the SID value on DASH targets using DASHConfig.

4. Add "john.h" to "LibrarySystems" group.

Appendix B - XML File example

```
<?xml version="1.0" encoding="utf-8" ?>
- <DASHPROVISIONSETTINGS>
  - <MANAGEMENTTARGET>
    - <GLOBAL>
        <ENABLEDASHTARGET>true</ENABLEDASHTARGET>
      - <HTTPS>
          <ENABLESUPPORT>true</ENABLESUPPORT>
          <TCPIPPORT>664</TCPIPPORT>
          <HTTPREALM>Broadcom Management Service</HTTPREALM>
        - <HTTPSTARGETTOCONSOLE>
            <CERTIFICATEPATH>DASHAD.cer</CERTIFICATEPATH>
          </HTTPSTARGETTOCONSOLE>
        - <HTTPSCONSOLETOTARGET>
            <CERTIFICATEPATH>DASHAD.cer</CERTIFICATEPATH>
          </HTTPSCONSOLETOTARGET>
        </HTTPS>
      - <HTTP>
          <ENABLESUPPORT>true</ENABLESUPPORT>
          <LIMITTODISCOVERY>true</LIMITTODISCOVERY>
          <TCPIPPORT>623</TCPIPPORT>
          <HTTPREALM>Broadcom Management Service</HTTPREALM>
        </HTTP>
      </GLOBAL>
    - <USERS>
      - <USER>
          <USERID>Administrator</USERID>
          <PASSWORD>adminpassword</PASSWORD>
          <ORGANIZATION>IT</ORGANIZATION>
          <ENABLE>true</ENABLE>
        - <ROLES>
            <ROLE>Administrator Role</ROLE>
          </ROLES>
        </USER>
      - <USER>
          <USERID>Auditor</USERID>
          <PASSWORD>readpassword</PASSWORD>
          <ORGANIZATION>IT</ORGANIZATION>
          <ENABLE>true</ENABLE>
        - <ROLES>
            <ROLE>Auditor Role</ROLE>
            <ROLE>Read Only Role</ROLE>
          </ROLES>
        </USER>
      </USERS>
    - <ACTIVEDIRECTORY>
        <ENABLESUPPORT>true</ENABLESUPPORT>
        <ACTIVEDIRECTORY_SPNACCOUNT>DASHSpnUser</ACTIVEDIRECTORY_SPNACCOUNT>
        <SPNACCOUNT_PASSWORD>spnpassword</SPNACCOUNT_PASSWORD>
      - <ACTIVEDIRECTORY_GROUPS>
        - <ACTIVEDIRECTORY_GROUP>
            <GROUPNAME>DASH Admins</GROUPNAME>
            <OBJECTSID>S-1-5-21-000000169-0004209000-0005141000-1155</OBJECTSID>
          - <ROLES>
              <ROLE>Administrator Role</ROLE>
            </ROLES>
          </ACTIVEDIRECTORY_GROUP>
        - <ACTIVEDIRECTORY_GROUP>
            <GROUPNAME>DASH Auditors</GROUPNAME>
            <OBJECTSID>S-1-5-21-000000169-0004209000-0005141000-1156</OBJECTSID>
          - <ROLES>
              <ROLE>Auditor Role</ROLE>
              <ROLE>Read Only Role</ROLE>
            </ROLES>
          </ACTIVEDIRECTORY_GROUP>
        </ACTIVEDIRECTORY_GROUPS>
      </ACTIVEDIRECTORY>
    </MANAGEMENTTARGET>
  </DASHPROVISIONSETTINGS>
```

Figure 7: XML file example

More Information

DASH forum
http://www.amd.com/DASH

How to configure Domain Controller in Windows Server
http://technet.Microsoft®.com/en-us/library/cc779648%28v=ws.10%29.aspx

How to extend the Active Directory schema for Configuration Manager
http://technet.Microsoft®.com/en-us/library/bb633121.aspx

MYITForum
http://www.myitforum.com

DASH Plug-in user manual and help file

The help file that gets installed with DASH Plug-in provides detailed information on support for role-based authorization in DASH Plug-in. The default location for the help file is:

'C:\Program Files (x86)\SCCM DASH Plug-in\SCCMDASHPlug-in.chm.

This information can also be found in the user manual document in the installer package.