Microsoft® Active Directory® Theory and Operation with the Dell™ Chassis Management Controller

This Dell technical white paper contains a business validated solution from Dell about the Dell Chassis Management Controller.

Dell | Product Group

Authors:

Bill Ashlock

This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

December 2012| Rev 1.0

Contents

Tables

Introduction

This document explains the process involved with Microsoft Active Directory successfully interacting with the Dell Chassis Management Controller.

The Dell Chassis Management Controller is used to manage the Enterprise Chassis environment.

Problem statement

In most deployments, Active Directory requires customization or updates because there are many pieces to configure, and these items may confuse users. The process is not intuitive, and there is no simple way to correctly configure these devices. This white paper offers information to help identify and eliminate configuration errors and installation problems, while explaining how to simplify the management of the Dell Chassis Management Controller in your current Microsoft Active Directory environment.

The pieces of the whole solution are scattered throughout different Dell and Microsoft documents. This makes the information difficult to find and put together to solve the problem of integrating Dell devices in to the Active Directory environment.

Praxis solution

This document combines all the pieces necessary to understand how the interaction of Microsoft Active Directory works with the Dell Chassis Management Controller.

Benefit 1	Helps you understand the products so you save time and enjoy an immediate return on your investment.
Benefit 2	Breaks down the complex setup and administration needed to support your environment. In addition, it supplies you with the theory behind how the setup works.
Benefit 3	Helps you plan the setup to use in your Windows® Active Directory environment.

Implementation

The following sections are broken down and organized into simple categories that let you go directly to the section you need, based on the information necessary to complete the setup task. Although it is recommended to read through each section, you can quickly find answers to the implementation questions for your environment. The following sections are organized by the theory and operation of Microsoft and Dell setup for the environments.

The theory of Active Directory

Microsoft Active Directory is an environment to manage users, computers, and devices. This is a central location to manage the permissions or security, and network administration of the objects stored in Active Directory. Microsoft Active Directory or Directory Services (DS) is a mapping system that lets you store these objects in a tree and assign permissions to them. You can then address or access these objects by name using the Lightweight Directory Access Protocol (LDAP) with Internet Protocol (IP). This lets you set permissions for users or computers, and communicate to these computers or validate

users using IP on your network back to the domain controller. Microsoft domain controllers are where you setup all of these services, protocols, and objects.

When you setup Microsoft Active Directory you must first install a Microsoft Windows Server 2003 or later, which is the only server software version currently supported by the Dell Chassis Management Controller environment. After the server is installed, you *turn* it into a domain controller using the built-in application *DCPromo*. This process promotes the server to a domain controller, and as part of this process you install a Domain Name System (DNS), Active Directory Domain, such as (yourcompany.com or a private address; your company.local).

DNS lets you access objects by names, and not the ID value associated with remembering a number. An example of this is Dell.com is translated to an IP address in a browser and returns you to the Web site by name. Installing a domain controller lets your company be identified as a name, and if you did not have DNS, you would have to remember numbers, IP addresses, such as 192.168.34.87. Internet Service Providers normally assign IP addresses to a network connection, and a good tool used in troubleshooting DNS problems on Windows systems, servers, and clients, is nslookup. To test the connection, enter a command at a CMD prompt; nslookup dell.com. The command returns the IP address for dell.com. Enter this IP address into your browser, and it returns the dell.com Web site.

(Example only, data subject to change)

```
nslookup dell.com

Non-authoritative answer:

Name:    dell.com

Addresses:  143.166.224.244

143.166.83.38
```

When DNS is set up, create a forward and reverse DNS record for your Dell Chassis Management Controller. Forward records hold the name of the Dell Chassis Management Controller and reverse DNS records hold the IP address of it. When troubleshooting DNS problems, always make sure that the forward and reverse records are returned from DNS.

Note: The commands: ‘nslookup name’ returns an IP address and the ‘nslookup ip address’ returns a name.

If you want to create a single sign-on or smartcard (SC) or (two factor authentication - TFA) environment, you must install cryptography, known as certificate services (CS) on the domain controller. CS lets you exchange certificates with the Dell Chassis Management Controller and the Active Directory domain. When you exchange certificates you are creating a two way trust system. The Active Directory domain controller trusts the device and the device trusts the Active Directory domain controller. You can secure the communication using the secure socket layer (SSL) protocol in your browser, when cryptography is installed. These two features use Kerberos; the Dell Chassis Management Controller is compatible with only DES-CBC-MD5 encryption. On Windows 7 and later workstations, this encryption must be enabled in the local computer policy. During the setup process for these features, create a *keytab file*. This file is uploaded into the Dell Chassis Management Controller, so that it can access the Active Directory domain.

The keytab file is created on the domain controller to map a basic user account to the device. This allows the Dell Chassis Management Controller to connect to DS to lookup other objects in the tree and to find the permissions allowed by the Dell Chassis Management Controller. Because all permissions are only managed in DS, in extended schema mode, the Dell Chassis Management Controller must have access to DS using LDAP.

The Operation of Dell Chassis Management Controller

There are two ways to integrate Active Directory with Dell Chassis Management Controller:

- Standard schema
- Extended schema

Standard schema

With the standard schema, permissions are managed on the Dell Chassis Management Controller and user groups are managed on the Active Directory domain. The extended schema lets you manage all the users, devices and permissions in Active Directory. The Dell Chassis Management Controller operating system is running a version of Linux. For this operating system to access the Active Directory domain, it must search LDAP in DS for permissions. This allows the Dell Chassis Management Controller a level of access to the domain and to grant user access to the Dell Chassis Management Controller based on these permissions. This is the purpose of the keytab file. The keytab file maps the user account in Active Directory to the device. This way the device can access Active Directory to lookup information, permissions, devices and users, all which have access to the Dell Chassis Management Controller.

Standard schema access setup uses a group on the Active Directory domain. This is also the easiest schema to setup for Active Directory users. All the users are added to the group in Active Directory, while the permissions are managed at the Dell Chassis Management Controller. Within the Active Directory group, you add Active Directory users that can access the Dell Chassis Management Controller. You can create five different groups in Active Directory. These groups map to five different groups on the Dell Chassis Management Controller, with a different set of permissions for each group. You do not need to add or update any schema objects to your Active Directory environment for this authentication scheme. This lets the Active Directory users in the group access the Dell Chassis Management Controller, based on the permissions of the group created on the Dell Chassis Management Controller. We have created four permission groups:

- Administrators
- Power users
- Guest users
- Custom groups

Do not add the same user to multiple Active Directory groups. The domain name you created is linked to the standard schema setup page on the Dell Chassis Management Controller. This is how the Dell Chassis Management Controller knows which domain to access. On the Dell Chassis Management Controller you add the domain and the group of user from Active Directory. When you enter the domain name, DNS translates the name to an IP address and uses this on the network to connect to the domain.

Your workstation must look up your domain name in DNS. Use an IP address to the domain, if you do not have DNS setup. It looks up the name of the group or groups in LDAP to find the user that is requesting access to the Dell Chassis Management Controller. If the user is in a group, the permissions are set according what permissions have been set on the Dell Chassis Management Controller, then the authentication to the Dell Chassis Management Controller occurs and access is granted.

Extended schema

All of the extended schema management occurs on the domain controller server in Active Directory > Users and Computers. Update the Active Directory schema with the tools from the OpenManage Server Administrator DVD (OMSA), to use the extended schema. You must have the schema administrator privilege to update the Active Directory schema. In additions, you must install the Active Directory Users and Computers plugin. This lets you see the new objects that were added to DS by the schema update.

Table 1. Folder Names and Installation Types Under the DVD folders: sysmgmt\ManagmentStation\support\OMActiveDirectory_Tools\

Folder name	Installation type
ITA7	IT Assistant version 7.0 or later
OMSA	Dell OpenManage Server Administrator
KVM	KVM devices
RAC3	RAC 3 (version 3)
Remote_Management	RAC 4, RAC 5, **Dell Chassis Management Controller**, and iDRAC on xx0x modular systems.
Remote_Management_Advanced	iDRAC on xx1x systems **Note**: Only iDRAC6 is supported on xx1x systems.

Microsoft Domain setup for both TFA and SSO

To setup the two factor authentication (TFA) and single sign on (SSO) environment requires the following:

Only TFA:

- Only Internet Explorer 7 and later is supported for these TFA environments.
- Smart card login should be working with Active Directory login on workstations for use with TFA and SSO.
    - Pintool is needed for earlier versions of Windows, See Microsoft article KB909520.
    - Windows 7 may require drivers for the smart cards and/or readers. Drivers can be obtained from: http://catalog.update.microsoft.com/v7/site/home.aspx.
    - You may also check with your vendor.
- Test Smart Card Login with Active Directory user, to make sure it works.
- Set up a Smart Card Enrollment Agent (workstation) to enroll smart card users for the domain.

Only SSO:

- Both browsers, FireFox 3.0+ and Internet Explorer 7.0+ must be configured to implement SSO. Changes of each browser are outlined below.
- Only the Internet Explorer browser IE7 and later are supported for SSO.

Both TFA and SSO:

- Microsoft Active Directory Domain controller with forest setup.
- Cryptographic service running on a Windows domain controller > Certificate Services.
- Dynamic Domain Name Service (DDNS). Set up both DNS forward and reverse zones.
- This allows your Dell Chassis Management Controller to be automatically added to the DNS zones. Alternatively, you can manually add the Dell Chassis Management Controller to both zones in DNS.
- User Workstations need to be part of the domain.
- Make sure the Active Directory user login works on the workstation.
- Make sure you have all the latest security patches and service packs installed on your version of Windows server.
- Install the latest version of KTPASS available from Microsoft Web site.
- Set Internet Explorer Security settings as follows:
    - Allow your DNS domain name that will be used with your device.
    - Allow your device IP address if you are not using the name for setup. After which, only use the DNS name of the device.
    - Allow Active X controls, plug-ins, and downloads. During the TFA login process you are presented with an Active X plug-in that needs to download and install in the IE browser.
    - Disable popup blocker. If you add the domain to the allow list in the IE browser options, then you can leave it turned on.
- All domain controllers and computers in the forest must trust the root Certification Authority (CA) of the smart card certificate's certificate chain.
- All domain controllers must have a Domain Controller or Domain Controller Authentication certificate installed. Smart card authentication requires mutual authentication of the user and the domain controller involved in the Kerberos authentication.
- The smart card certificate must contain the Smart Card Logon, (1.3.6.1.4.1. 311.20.2.2) and Client Authentication (1.3.6.1.5.5.7.3.2) object identifier (OID) in the Enhanced Key Usage (EKU) extension or in the Application Policies extension. The Smart Card Logon and Client Authentication OIDs must be valid in the entire certificate chain. This is part of the cryptography install process from Microsoft.
- Include the CA that issues the smart card certificate in the Active Directory NT Authority (NTAuth) store. When a CA certificate is added to the NTAuth object in Active Directory (CN=NTAuthCertificates, CN=Public Key Services, CN=Services,

CN=Configuration, DC=ForestRootDomain, where ForestRootDomain is the LDAP distinguished name of the forest's root domain), the thumbprint of the CA's certificate is automatically distributed to all Windows 2000 and later domain members in the HKEY_LOCAL_MACHINE\Software\ Microsoft\EnterpriseCertificates\NTAuth\ Certificates registry key. You can verify the CA certificates included in the NTAuth store by using the PKI Health Tool (pkiview.msc) included in the Windows Server 2003 Resource Kit.

Configuring the SSO browser

- Internet Explorer - Set your browser to include the domain in options. Open IE Options, click the Security tab, click Local Intranet, click Sites > Advanced, and add the domain. For example: *.dell.lab. Some IE browsers require you to *Enable integrated Windows Authentication*. Go to the Advanced tab, scroll down under Security, and select the check box.
- FireFox - Open the browser and enter about:config in the address bar. Search or enter in the filter *network.automatic-ntlm-auth.trusted-uris*, enter your domain (for example: dell.lab) by double clicking the line, and then press Ok to save.

Summary

This white paper lets you reference information in one place, helps you save time on implementing solutions in your environment, troubleshoots problems that may occur, and helps you to administer Dell devices.