Kerberos™-Based Active Directory® Authentication to Support Smart Card and Single Sign-On Login to DRAC5

A Dell™ Technical White Paper

Dell OpenManage™
Systems Management

By Austin Cherian

Dell Product Group

April 2009

TABLE OF CONTENTS

Introduction

Given the industry trend of using directory services for central management of user access to enterprise resources, Dell™ Remote Access Controller (DRAC) 5 supports Microsoft® Active Directory (AD) user name and password credentials to enable a DRAC session. To enable stronger authentication standards, DRAC 5 now supports Kerberos-based AD authentication to support AD smart card and single sign-on logins.

Kerberos is a network authentication protocol that allows systems to communicate securely over a non-secure network by allowing the systems to prove their authenticity.

Starting with DRAC 5 version 1.40, DRAC 5 supports two types of Kerberos authentication mechanisms:

- AD single sign-on
- AD smart card login.

To enable single-sign-on, DRAC 5 uses the Kerberos-specific credentials cached in the operating system after the user has logged in using a valid AD account. To enable smart card login, DRAC 5 uses smart card-based two factor authentication (TFA) as credentials to enable an AD login. This is a follow-on feature to the local smart card authentication released in DRAC 5 version 1.33.

DRAC 5 Kerberos Configuration

To support the two new authentication mechanisms, DRAC 5 can be configured as a Kerberos-based service on a Windows® Kerberos network. The DRAC 5 Kerberos configuration uses the same steps as configuring a non-Windows Kerberos service as a security principal in the server AD.

The Microsoft tool ktpass, supplied as part of the server installation CD, is used to create Service Principal Name (SPN) bindings to a user account and to export the trust information into a Kerberos "keytab" file. This file enables a trust relationship between an external user or system and the Key Distribution Centre (KDC). The keytab file contains a cryptographic key that is used to encrypt the information between the server and the KDC. The ktpass tool allows the UNIX-based services that support Kerberos authentication to use the interoperability features provided by a Windows server Kerberos KDC service.

The keytab file obtained from the ktpass utility is sent to DRAC 5 as a file upload, and enables DRAC 5 to be configured as a Kerberos service on the network. The following steps outline how to create a keytab file and upload it to DRAC 5.

1. Create a user account in AD that will be used to map a DRAC 5 to an AD service principal. For the user name, either use a name that is convenient or use the registered DNS domain name of the DRAC 5. For example, if the DRAC 5 to be configured has a DNS entry of drac1950.domain.com, create a new user in AD called drac1950.
2. On the user account properties, enable the following settings:
   - Do not require Kerberos pre-authentication
   - Use DES encryption types for this account
3. Use the ktpass command to create the Kerberos keytab file (krbkeytab). For example, use the following ktpass command to create the Kerberos keytab file:

   ```
   C:\>ktpass -princ HOST/dracdnsname.domainname.com@DOMAINNAME.COM -
   mapuser <username> -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -
   pass * -out
   c:\krbkeytab
   ```

   `<username>` is the user name of the user account created in step 1. The encryption type that DRAC 5 uses for Kerberos authentication is DES-CBC-MD5. The principal type is KRB5_NT_PRINCIPAL.

   The ktpass command will result in the mapping of the DRAC SPN, HOST/dracdnsname.domainname.com, to the user account created in step 1, and will also generate the keytab file that contains the encryption key.
4. Upload the keytab to DRAC 5 using the GUI or RACADM commands. To upload using the GUI, use the following steps:
   a. Login to DRAC 5.

b. Navigate to the Kerberos Keytab upload page: **Remote Access**-> **Configuration** -> **Active Directory** -> **Kerberos Keytab Upload**
c. Click the **Browse** button and browse to the location of the Keytab file to select it, or type the path of the Keytab file directly into the text box.
d. Click **Upload**.

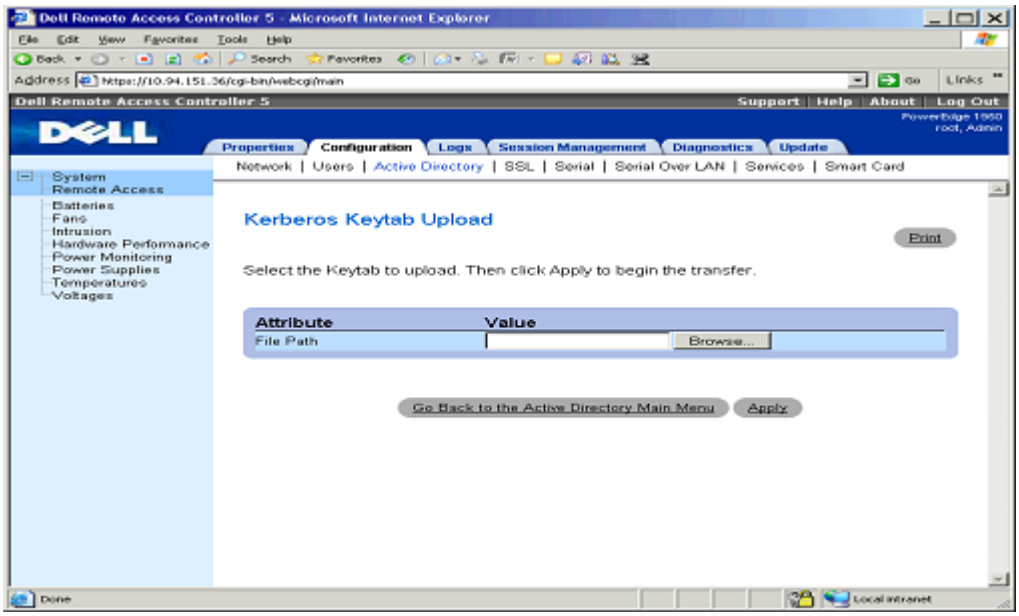

Figure 1: Kerberos Keytab Upload Windows

To upload the file using a RACADM commands, enter the following command:

```
racadm krbkeytabupload –f <filename>
```

Where `<filename>` is the name of the Keytab file. This RACADM command is supported by both local and remote RACADM.

Configuring DRAC 5 Active Directory Users for Single Sign-On Logon

Before configuring the AD single sign-on feature, ensure that you have configured the DRAC 5 for AD logins. The domain user account you will use to login into the system must be enabled for DRAC 5 AD login as well. Make sure to enable the AD logon setting; see "Using the DRAC 5 With Microsoft Active Directory" in the DRAC 5 User's Guide for more information on how to set up AD users. You must also enable the DRAC 5 as a Kerberos service by uploading a valid keytab file, obtained after running the ktpass command, to the DRAC 5 as described in the previous section of this document.

Use the following steps to enable AD single sign-on using the DRAC 5 GUI:

1. Login to DRAC 5.
2. Navigate to the **Active Directory Configuration and Management** page: **Remote Access** -> **Configuration** -> **Active Directory** -> **Configure Active Directory**
3. On the **Active Directory Configuration** page, select the “Enable Single Sign-On” option. Single sign-on logins are now enabled.

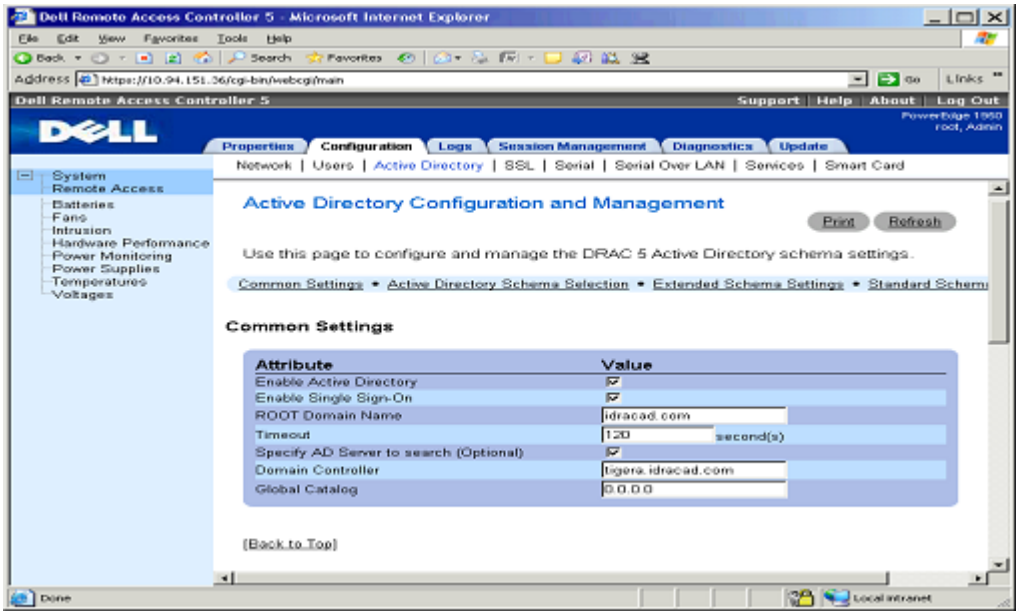

Figure 2: Active Directory Configuration and Management Window

To enable single sign-on logins using the command line, enter the following command:

```
racadm –g cfgActiveDirectory –o cfgADSSOEnable 1
```

Logging Into the DRAC 5 Using Single Sign-On

Client single sign-on authentication involves downloading a plug-in from the DRAC web login page and installing it on the client. To ensure proper installation of the plug-in, you must have the latest Visual C++® 2005 runtime components. For more information, see the Microsoft Web site. This feature is currently supported on 32-bit Windows operating systems. Use the following steps to log into DRAC 5 using single-sign on:

1. Login to your system using a valid AD account.
2. Enter the Web address of the DRAC 5 in the address bar of your browser. Depending on browser settings, you may be prompted to download and install the Single Sign-On ActiveX® plug-in when using this feature for the first time.

You are logged into DRAC 5 with the appropriate privileges if:

a. You are an AD user.
b. You are configured in DRAC 5 for AD login.
c. DRAC 5 is enabled for Kerberos AD authentication.

Configuring AD Users for Smart Card Logon

AD smart card login to DRAC 5 is a follow-on feature to the supported local smart card login. For more information on the local smart card feature, see “Configuring Smart Card Authentication” in the DRAC 5 User’s Guide.

Before using the AD smart card login feature, make sure that you have configured the DRAC 5 for AD login and that the user account issued the smart card has been enabled for DRAC 5 AD login. Also ensure that you have enabled the AD login setting. See "Using the DRAC 5 With Microsoft Active Directory" in the DRAC 5 User’s Guide for more information on how to set up AD users. You must also configure DRAC 5 as a Kerberos service by uploading a valid keytab file, obtained after running the ktpass command, to DRAC 5 as described in the section DRAC 5 Kerberos Configuration in this document. Use the following steps to enable smart card login using the DRAC 5 GUI:

1. Login into the DRAC GUI.
2. Expand the System tree and click **Remote Access**.
3. Click the **Configuration** tab and then click **Smart Card**.
4. Configure the smart card logon settings.

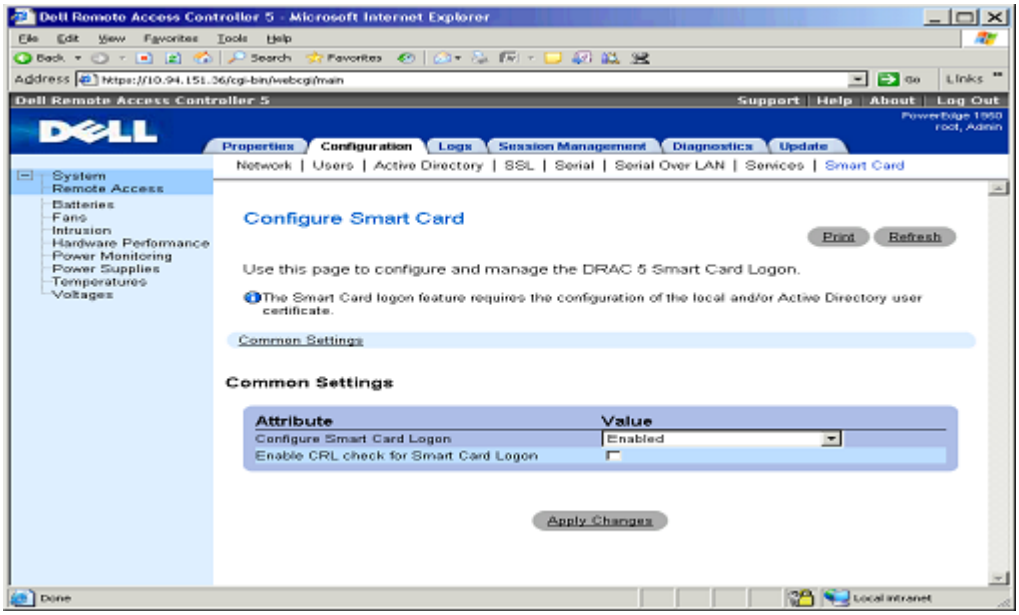

Figure 3: Configure Smart Card Window

If the **Configure Smart Card Logon** attribute is set to **Enable** or to **Enable with Remote Racadm**, the DRAC 5 GUI login will prompt the user to insert the smart card and enter in the smart card PIN. The **Enable** option disables CLI out-of-band interfaces that support only single-factor authentication—such as Telnet, Secure Shell (SSH), serial consoles, remote RACADM, and Intelligent Platform Management Interface (IPMI) Over LAN. The **Enable with**

Remote Racadm option disables the same set of interfaces, but leaves remote RACADM enabled.

5. Click **Apply Changes**.

Logging Into DRAC 5 Using a Smart Card

Verify that the smart card is supported by the Microsoft Windows operating system. Windows supports a limited number of smart card cryptographic service providers (CSPs) out of the box; unsupported smart cards require administrators to install the appropriate CSPs provided by the smart card vendor.

The AD smart card client authentication involves downloading a plug-in from the browser and installing it on the client. For proper installation of the plug-in, ensure that you have the latest Microsoft Visual C++ 2005 runtime components. For more information, see the Microsoft Web site. This feature is only supported on 32-bit Windows operating systems. Use the following steps to log into DRAC 5 using a smart card:

1. Access the DRAC 5 Web page..The DRAC 5 login page appears prompting you to insert the smart card. You may be prompted to download and install the Smart Card ActiveX® plug-in when using this feature for the first time.
2. Insert the smart card into the reader and enter the smart card PIN.
3. Click Login.

You are logged into DRAC 5 with appropriate privileges if:

a. You are a Microsoft AD user
b. You are configured in DRAC 5 for AD login
c. DRAC 5 is enabled for Kerberos AD authentication

Advanced Enterprise class security standards

The security features outlined in this paper provide the flexibility to deploy DRAC 5 into an existing enterprise’s security architecture in a seamless fashion. It provides existing users with the option of authenticating with the remote access solution in a similar manner as they would authenticate with any other access restricted enterprise resources using advanced authentication standards, such as two-factor authentication and single sign on. DRAC 5 is now more in line with industry standard authentication solutions with the introduction of these features.