iDRAC6

Integrated Dell™ Remote Access Controller 6 Security

Version 1.0
July 2010

Table of Contents

Introduction

The Integrated Dell Remote Access Controller 6 (iDRAC6) is designed to improve the overall availability of Dell servers and to help system administrators save time. The iDRAC6 achieves this by alerting administrators to server problems, enabling remote server management and reducing the need for the administrator to physically visit the server.

The iDRAC6 can help improve an administrator's ability to manage a server without having physical access to the server, even when it is not operational. This can help administrators in the following ways.

1. Increased Availability – Early notification of potential or actual failures can help prevent a server failure or reduce recovery time in the case of a failure.
2. Improved Productivity and Lower TCO – Extending the reach of administrators to larger numbers of distant servers can make IT staff more productive while driving down operational costs such as travel.
3. Enhanced Embedded Management via Lifecycle Controller – Lifecycle Controller provides local deployment and simplified serviceability via Unified Server Configurator and WSMan interfaces for remote deployment integrated with Dell Management Console and other consoles.
4. Secure Environment – By providing secure access remote servers, administrators can carry out critical management functions while maintaining server and network security. *This is the topic explored by this whitepaper.*

Unlike the DRAC5, the iDRAC6 is available in three flavors: iDRAC6 Express, iDRAC6 Enterprise, and the vFlash option for iDRAC6 Enterprise. While the iDRAC6 Express offers a rich feature set, iDRAC6 Enterprise extends this feature set with more advanced remote access features. The vFlash option for iDRAC6 Enterprise enables still more automation features including virtual flash partitions and advanced Lifecycle Controller features. Each version of iDRAC6 provides secure access to its feature set.

Because iDRAC6 is a networked-attached device with powerful management features, securing the iDRAC6 interfaces is of paramount importance. This whitepaper explores how security is built-in to the iDRAC6 hardware and software design so IT administrators can spend more of their time on productivity than security concerns.

Physical connections to iDRAC

When considering the security of a device it is helpful to visualize its physical connections within the system. Figure 1 illustrates the iDRAC6 processor and how it integrates with its physical environment. It is a 220 MHz System on a Chip (SOC) using 128 MB of RAM. For nonvolatile storage it has access to an EEPROM whose size is dependent on the server model, a 1 GB eMMC card (for the Life Cycle Controller), and optionally a 1 GB SD card (vFlash). The bootloader and configuration for the iDRAC6 is stored on the EEPROM, and the primary firmware image is stored on the eMMC card for 200-900 series servers.

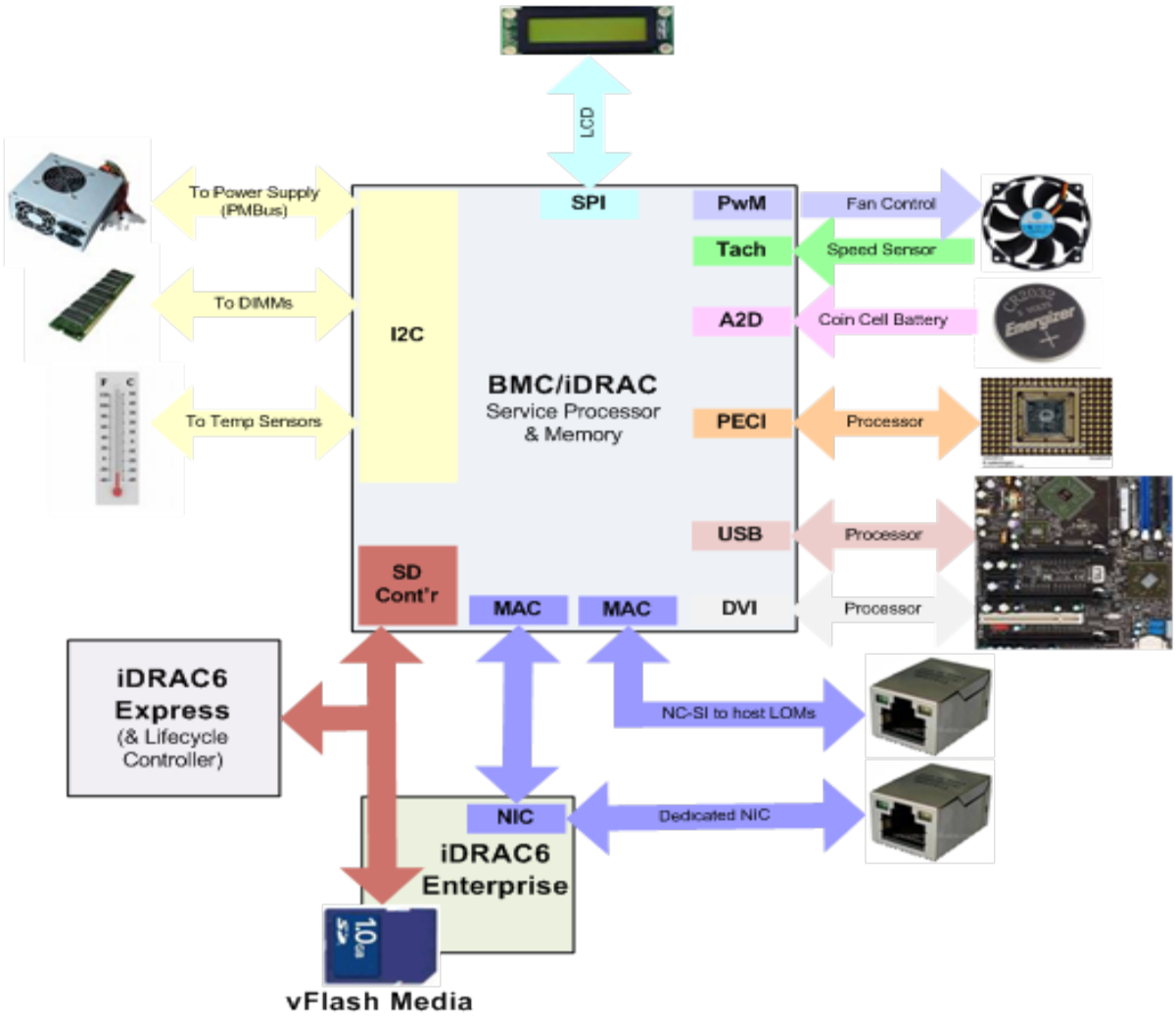

Figure 1 iDRAC physical connections

Access to iDRAC6 from a local user of the server is assumed to be mitigated by operating system authentication as mentioned later in this paper. The primary focus of security measures is to prevent attacks from remote users through a network.

As shown in the picture, there are two possible ways to connect the iDRAC6 to a network. First, the iDRAC6 is accessible over the same network as the server's embedded NIC interfaces. This is called the "Shared NIC" and is described in the next section. Second, the iDRAC6 Enterprise card is an orderable option for iDRAC6 and provides a dedicated management port that is used only by the iDRAC6. One advantage of the dedicated port is to contain all management traffic on an isolated network with no effect on the bandwidth of the server's network ports. Another potentially more important advantage can be that it provides iDRAC6 isolation for security purposes for servers behind a firewall and directly accessible from the internet. The disadvantage of the dedicated NIC is additional cabling.

Broadcast and multicast protection are provided in the iDRAC6 software. If a threshold number of received packets are reached within a short period of time, the iDRAC6 turns on broadcast and multicast

filtering. This feature is active with both the shared and dedicated network modes and provides protection against a denial of service attack. In addition, there is internal firewall software as described by the IP blocking and IP range filtering in subsequent sections.

Shared NIC Mode

Figure 2 provides more detail about the connection between the iDRAC6 and the network adapter. Incoming packets are filtered by the MAC address of the iDRAC6. If there is a match, the packet is routed to the sideband connection to iDRAC6. Otherwise, the packet is filtered and is not received by iDRAC6. Outgoing packets from the iDRAC6 are sent onto the network, but it is physically impossible to send a packet through the network adapter to the host processor. This is also the case for outgoing packets; it is not possible to send a packet to the iDRAC6 through the network adapter. This isolation provides security by preventing access to one network even if the other is compromised.

The iDRAC6 uses the high-speed NC-SI (Network Controller Sideband Interface) to communicate with the network controller. The iDRAC6 configuration allows the user to select between the dedicated port, the shared port ("network controller" in Figure 2, or LAN on motherboard), the shared port with failover to LOM2 (LAN #2 on motherboard), or the shared port with failover to all LOMs. These options provide significant flexibility to the user while maintaining the security discussed in this section.

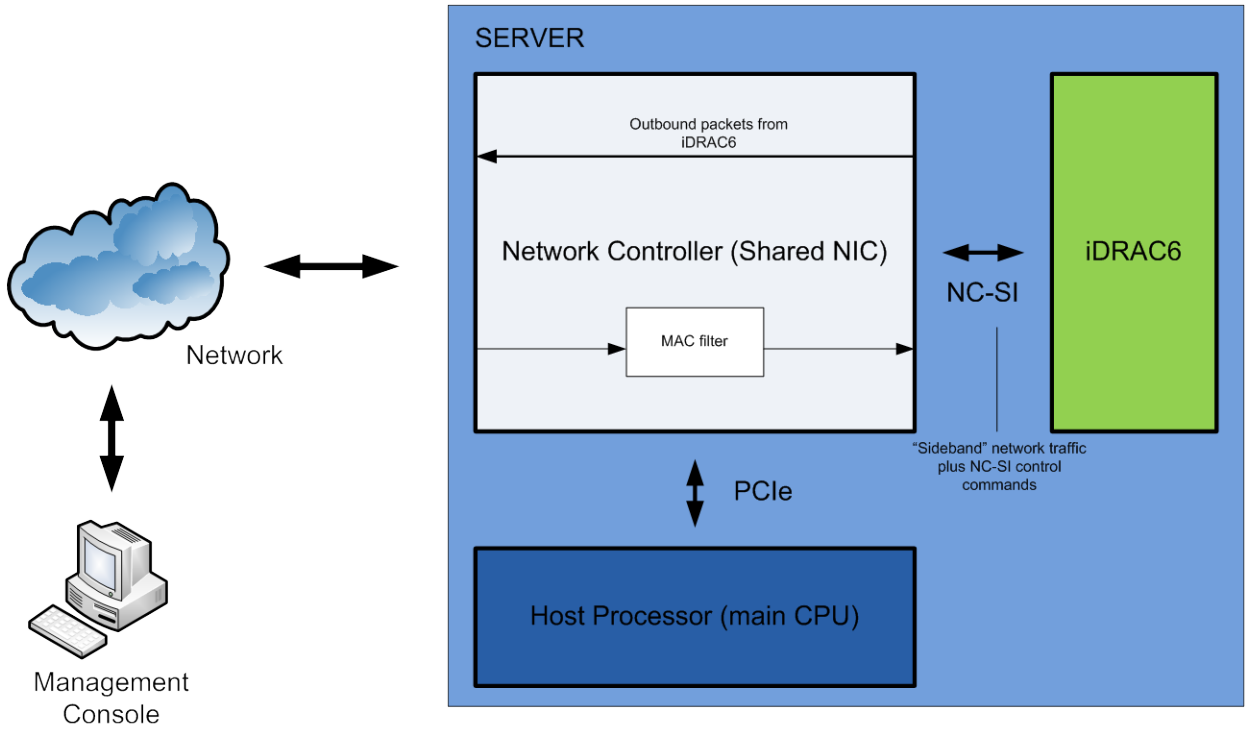

Figure 2 – NC-SI sideband interface

User Authentication and Authorization

Local Accounts

By default the iDRAC6 is configured with a local administrator account. This default user name is "root" and the password is "calvin". The default user allows users to access the iDRAC6 after it arrives in their environment. Dell highly recommends that this user account is secured after arriving in the user environment. The iDRAC6 supports up to 16 local users each of which can be enabled or disabled.

Alternatively, iDRAC6 can be secured by disabling all local user accounts and using only Microsoft® Active Directory® users since Active Directory is considered to have stronger secure policy management. LDAP is also supported for customers that want to use directory services instead of local username and password accounts. This is advantageous because it provides a central location for managing authorized user accounts instead of requiring maintenance of accounts on individual machines in large installations. These are described in subsequent sections.

- Local usernames and passwords can be changed using all of the iDRAC6 secured interfaces (i.e. web interface, command line, and WSMAN interface). The iDRAC6 local user accounts have the following restrictions. Anonymous users are not supported
- NULL user name are not supported
- NULL password are not supported
- Maximum username length is 16 characters
- Maximum password length is 20 characters

The iDRAC6 local user account information is stored on NVRAM and is encrypted via a proprietary algorithm.

The iDRAC6 supports privilege-based access to iDRAC6. Every local user or Active Directory user has a privilege set associated with it. The privileges available to users are highly configurable and are documented in the user guide.

1. IPMI user privileges
    a. Maximum LAN User Privilege Granted.
    b. Maximum Serial Port User Privilege Granted
    c. Enable Serial Over LAN Allows the user to use IPMI Serial Over LAN.
2. iDRAC6 user privileges
    a. Login to iDRAC6
    b. Configure iDRAC6
    c. Configure Users
    d. Clear Logs
    e. Execute Server Control Commands
    f. Access Console Redirection
    g. Access Virtual Media
    h. Test Alerts
    i. Execute Diagnostic Commands

The users' roles can be configured as administrator, operator, read only, or none. This role defines the maximum privileges available. Operator privileges can be individually configured. The user guide provides further explanation of these roles and privileges. Dell recommends restricting privileges to the minimum needed by individual users. There is much flexibility that could be used for different levels of administrative maintenance.

Smart Card

One enhanced security measure currently under adoption in many enterprise data centers is two-factor authentication. Two-factor authentication is based on both an object and device (such as a smart card or USB key) and specific knowledge (such as a PIN or password). Standard single-factor authentication is based only on specific knowledge.

The iDRAC6 allows login via Smart Card authentication for local users. After Smart Card login is enabled, the iDRAC6 login page will prompt the user to insert a smart card and enter the PIN. When the user clicks the login button the user is authenticated based on the Smart Card and the PIN credentials entered.

Before enabling the smart card logon feature, administrators should first configure local iDRAC6 users for smart card logon. Local users can be enabled in the iDRAC6 graphical user interface (GUI) by selecting Remote Access > Configuration > Users, then selecting from the configurable users available. Two-factor authentication can also be used for Active Directory users.

When enabling a user for smart card logon, administrators should upload the user's smart card certificate and the trusted Certificate Authority (CA) certificate to the iDRAC6. The user certificate can be obtained by exporting the smartcard certificate using the card management software from the smart card vendor into a Base64-encoded file. This file can be uploaded to the iDRAC6 as the user certificate. The trusted CA that issues the smart card user certificates typically also exports the CA certificate to a Base64-encoded file, which administrators can then upload to the iDRAC6. Administrators should configure each user with the username that matches the user principal name in the smart card certificate. For example, for a smartcard certificate issued to sampleuser@domain.com, administrators should use "sampleuser" as the username.

Administrators can enable smart card logon in the iDRAC6 GUI by selecting the Remote Access menu item followed by the Configuration tab and Smart Card section. If the Configure Smart Card Logon attribute is set to Disabled, the system prompts for a username and password when users attempt to log in through the GUI or through a command-line interface (CLI). If this attribute is set to Enable or to Enable with Remote RACADM, the system prompts for a smart card when users attempt to log in through the GUI. Other interfaces that do not support smart cards are automatically disabled. The Smart Card enable setting 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 setting disables the same set of interfaces but leaves remote RACADM enabled. Typically, administrators should use the

Enable setting, reserving the Enable with Remote RACADM setting for iDRAC administrators needing to access the iDRAC6 to run scripts using remote RACADM commands.

After administrators have configured smart card logon for local iDRAC6 and Microsoft Active Directory users and enabled the smart card logon feature, the iDRAC6 GUI displays the smart card login page when users attempt to access the iDRAC6. If the Microsoft ActiveX® smart card reader plug-in is not present on the user's client system, the system prompts them to download and install it before continuing. After the smart card is inserted into the reader, and the login link is clicked, the IDRAC 6 prompts them for the smart card PIN.

If the user enters the correct PIN, the IDRAC 6 verifies the user's private key on the smart card, the validity of the digital signature of the certificate, the certification chain from the trusted CA, and the expiration date of the certificate. It also confirms that the user administrators to install the appropriate CSPs provided by the smart card vendor. Administrators can check whether smart card CSPs are present on a particular client by inserting the smart card in the reader at the Windows login screen (accessed by pressing Ctrl+Alt+Del) and determining whether Windows detects the smart card and prompts for the PIN. They can also try to log in to Windows using the smart card.

Currently, this feature is supported only on Microsoft Windows clients using Microsoft Internet Explorer 6 and later.

Active Directory with Dell Schema Extension

A directory service maintains a common database of all information needed for controlling users, computers, and printers on a network. If your company uses the Active Directory service software, you can configure the software to provide access to the IDRAC6 allowing you to add and control IDRAC6 user privileges to existing users in the Active Directory software.

The Active Directory data is a distributed database of Attributes and Classes. The Active Directory schema includes the rules that determine the type of data that can be added or included in the database. The user class is one example of a Class that is stored in the database. Some example user class attributes can include the user's first name, last name, phone number, and so on. Companies can extend the Active Directory database by adding their own unique Attributes and Classes to solve environment-specific needs. Dell has extended the schema to include the necessary changes to support remote management Authentication and Authorization. To provide the greatest flexibility in a variety of customer environments, Dell provides a group of properties that can be configured by the user depending on the desired results. Dell has extended the schema to include Association, Device, and Privilege properties. The Association property is used to link together the users or groups with a specific set of privileges to one or more RAC (Remote Access Controller) devices. This model provides an Administrator with maximum flexibility over the different combinations of users, RAC privileges, and RAC devices on the network without adding too much complexity.

The iDRAC6 authenticates against Active Directory using LDAP simple binding and queries Active Directory objects via an SSL channel. All data including user name and password for authentication are

sent via an encrypted channel to Active Directory. When iDRAC6 establishes an SSL connection with Active Directory Domain Controller, it verifies the Domain Controller entity via SSL server authentication. The root CA SSL certificate (which is used to sign all the Domain Controller SSL certificates) has been imported to the iDRAC6. The iDRAC6 supports up to a 4096-bit root CA certificate and Domain Controller SSL certificate.

NOTE: Dell strongly recommends following the Microsoft PKI best practices and using 4096-bit for the root CA certificate and a 1024-bit for the Domain Controller certificate.

For an Active Directory user to have authority to access an iDRAC6, this user object or group has to be added to the Dell Association object. A Dell privilege object with the right privilege setting also needs to be added to the Dell Association object. Finally, a Dell RAC device object which represents iDRAC6 is added to Dell Association object. The RAC device object name has to be configured to that iDRAC6.

The basis for searching Active Directory to authenticate and authorize the RAC User will be that there is a member-memberOf relationship on the Association Object. Every member of a Group has a corresponding Linked Attribute member called memberOf that is part of the User Class. When we authenticate a user with LDAP, we can get the memberOf Attribute that will contain all of the Groups that this user is a member of. We can then walk through these groups until we arrive at our dellAssocationObject class.

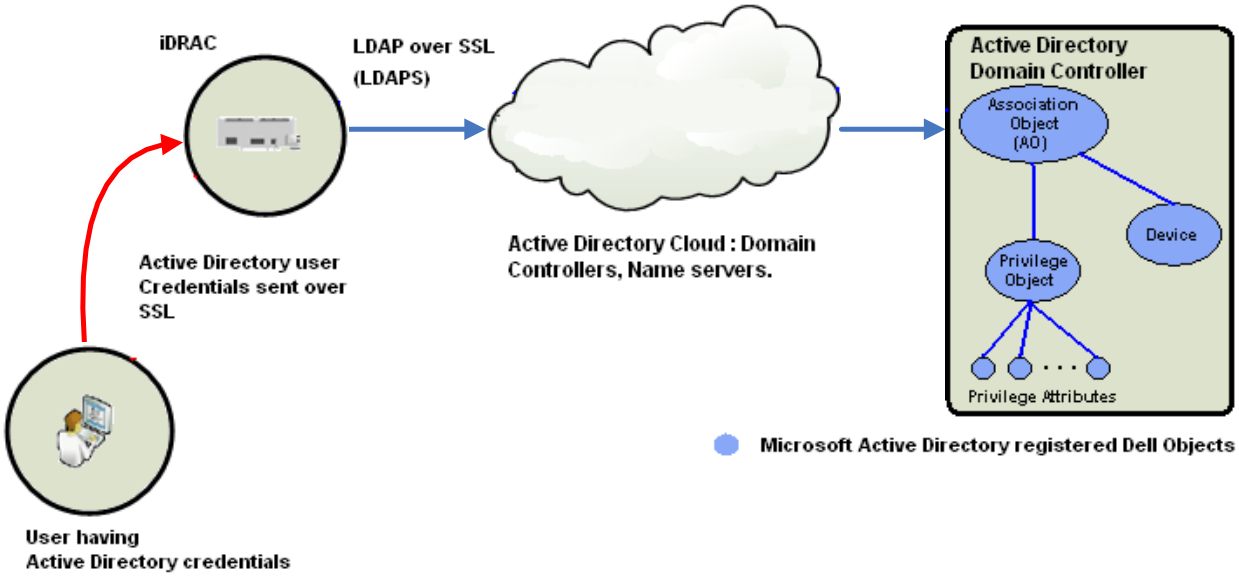

Figure 3 Use of Extended Schema

Note that the user could be a member of multiple association object classes, so we must take this into account in our query. When we find the dellAssocationObject Class that this user is a member of, we will then access the dellProductMembers attribute and walk this in the reverse order to determine if the

RacDevice, from which we are authenticating, is part of this attribute. Note that the dellProductMembers can be groups of RACs and will retain the aforementioned member-memberOf relationship. So, we will walk the list using the Member attribute for all of the groups that are in the list. If we find the name of the RAC Device that we are authenticating in the list, then we have authenticated the user and all we need to do is read the dellPrivilegeObject attributes and return them to the RAC as the authorization data (Privileges).

Active Directory Standard Schema

This requires iDRAC6 version 1.20 or later. The schema-extending solution provides maximum flexibility to the user but may be intimidating to some customers because the schema extension is not reversible. To meet the requirements from those customers who do not want to extend their existing Active Directory schema, Dell provides a standard schema solution in addition to the schema extension. This solution will provide the same flexibility of the current schema-extending solution and will allow granting different users different privileges on iDRAC6. The difference is that all the objects used in the standard schema solution are standard Active Directory objects while the schema-extending solution adds Dell objects to the users' Active Directory. The basic authentication and SSL connection are the same as they are with the Dell schema extension solution.

Instead of using the Dell Association object, Dell privilege object, and RAC device object to link a user, a standard group object has been used as a role group object. Any users in that role group have assigned privileges on certain iDRAC6 cards. The privilege of that role group has been defined in each individual iDRAC6 configuration database illustrated in Figure 4. Different iDRAC6 cards can give the same role group object different privileges.

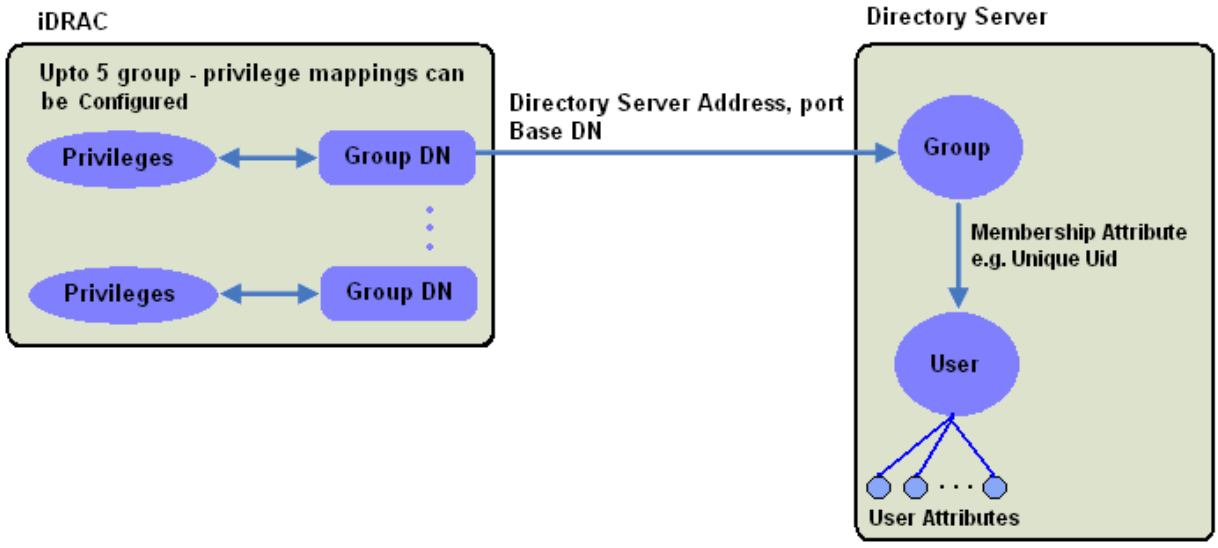

Figure 4 Active Directory Configuration Database

Single Sign On (SSO)

iDRAC6 allows a user configured in the Active Directory with Standard Schema to log in directly to the iDRAC6 GUI without explicitly providing login credentials. This feature is referred to as Single Sign-On (SSO) and it uses AD authentication along with Kerberos Network Authentication Protocol. Kerberos is a network authentication protocol that provides protection against eavesdropping and replay attacks (see further reading).

To be able to use SSO, the management station must belong to the same domain as configured in the Active Directory of the iDRAC6. The user logging into the management station must have login privileges to the domain and must be configured in the Active Directory. The iDRAC6 time must be within a plus or minus 5 minute range of the Domain Controller's time and in the same time zone. Upon opening the iDRAC6 GUI in a web browser, the user gets automatically logged into the iDRAC6 GUI using Kerberos Authentication.

Kerberos Authentication makes use of a Kerberos Client that gets downloaded to the management station as an Active X Plug-in. The client communicates with the Key Distribution Center (Active Directory Server) using Kerberos Protocol to validate the user. The KDC communicates with the iDRAC6 using AD queries to get user permissions. The KDC returns a Service Ticket to the client which is sent to the iDRAC6. The iDRAC6 validates the service ticket and if found to be valid binds to the AD server using a keytab file. If the user has sufficient privileges, the user is logged into the iDRAC6. Figure 5 demonstrates the Kerberos Authentication that takes place for SSO.

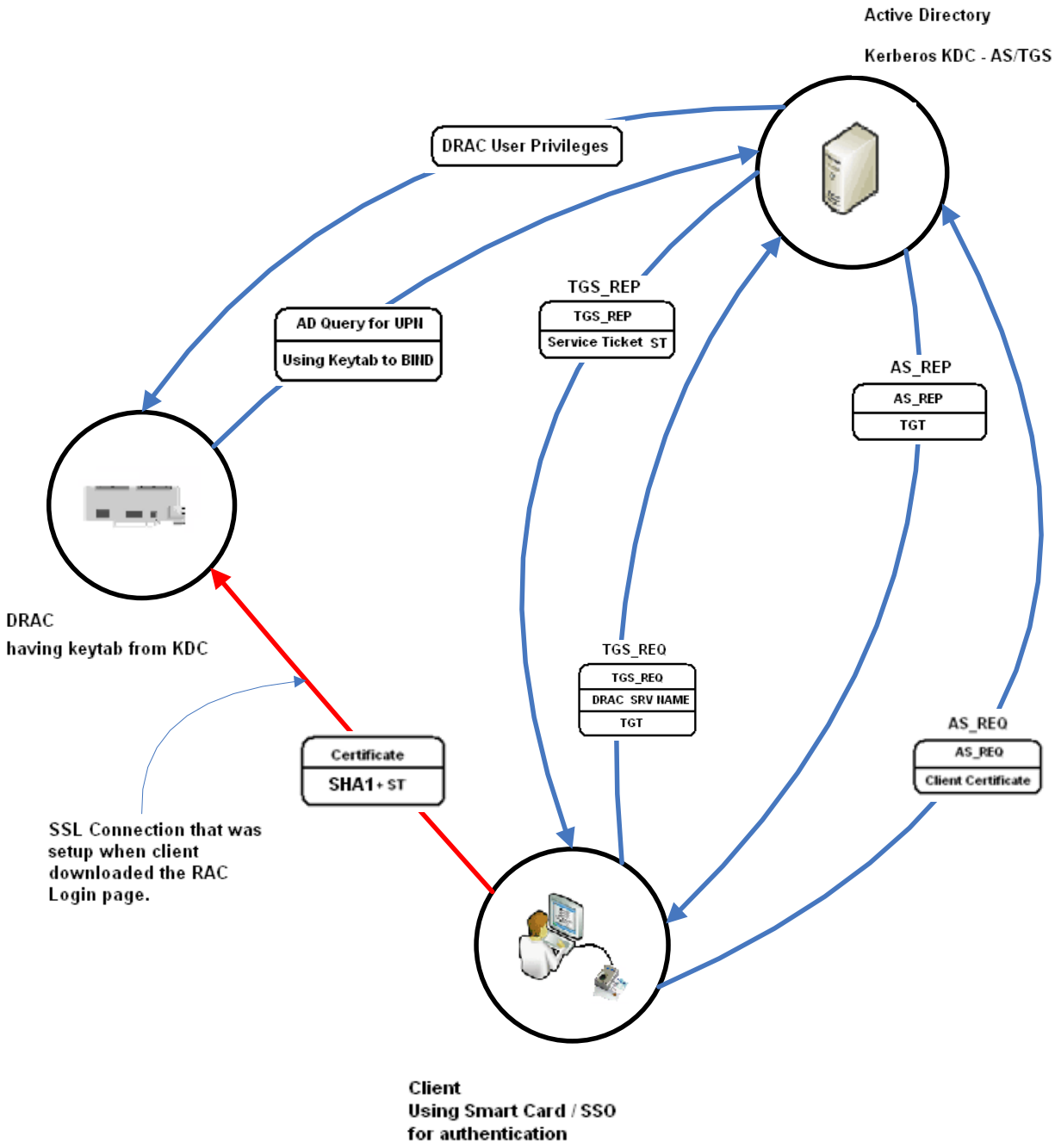

Figure 5 Log in via Active Directory with Smart Card (TFA)

Smart Card Authentication that uses the AD standard schema authentication is referred to as Two Factor Authentication. *TFA uses the same Kerberos Authentication procedure as used in Single-Sign On.*

Active Directory login troubleshooting

If you want to verify whether your configuration works, or if you need to diagnose the problem with your failed Active Directory login, you can test your settings from the iDRAC6 Web-based interface.

After you finish configuring settings in the iDRAC6 Web-based interface, click Test Settings at the bottom of the page. You will be required to enter a test user's name (for example, username@domain.com) and password to run the test. Depending on your configuration, it may take some time for all of the test steps to complete and display the results of each step. A detailed test log will display at the bottom of the results page.

Log in via Generic LDAP Directory services

The iDRAC6 provides a generic solution to support Lightweight Directory Access Protocol (LDAP) based authentication. This feature does not require any schema extension on the site directory services. To make the iDRAC6 LDAP implementation generic, the commonality between different directory services is utilized to group users and the map the user-group relationship. The directory service specific action is the schema. For example, they may have different attribute names for the group, user, and the link between the user and the group. These actions can be configured in iDRAC6.

The Generic LDAP feature is similar to the schema-less Active Directory login support; a standard group object has been used as a role group object. Any users in that role group have assigned privileges on certain a iDRAC6. The privilege of that role group has been defined in each individual IDRAC 6 configuration database. Different iDRAC6 controllers can give the same role group object different privileges.

Public Key Authentication over SSH

iDRAC6 supports the Public Key Authentication (PKA) over SSH. This authentication method improves SSH scripting automation by removing the need to embed or prompt for a user ID/password.

Up to four public keys can be configured per user that can be used over an SSH interface. Before adding or deleting public keys, ensure that you use the view command to see what keys are already set up, so a key is not accidentally overwritten or deleted. When the PKA over SSH is set up and used correctly, you do not have to enter the username or password when logging into the iDRAC6. This can be very useful for setting up automated scripts to perform various functions. This feature can be managed with RACADM and also from the GUI. When adding new public keys, ensure that the existing keys are not already at the index where the new key is added. iDRAC6 does not perform checks to ensure previous keys are deleted before a new one is added. As soon as a new key is added, it is automatically in effect as long as the SSH interface is enabled.

Generating Public Keys

Before adding an account, a public key is required from the system that will access the iDRAC6 over SSH. There are two ways to generate the public/private key pair: using PuTTY Key Generator application for

clients running Windows and ssh-keygen CLI for clients running Linux. The ssh-keygen CLI utility comes by default on all standard installations.

Logging in Using Public Key Authentication

After the public keys are uploaded, the user can log into the iDRAC6 over SSH without entering a password. The user also has the option of sending a single RACADM command as a command line argument to the SSH application. The command line options behave similar to remote RACADM since the session ends after the command is completed.

Encryption

Secure Sockets Layer (SSL)

The iDRAC6 includes a Web server that is configured to use the industry-standard SSL security protocol to transfer encrypted data over the Internet. Built upon public-key and private-key encryption technology, SSL is a widely accepted technique for providing authenticated and encrypted communication between clients and servers to prevent eavesdropping across a network.

An SSL and TLS (Transport Layer Security) enabled system:

- Authenticates itself to an SSL-enabled client
- Allows the client to authenticate itself to the server
- Allows both systems to establish an encrypted connection

This encryption process provides a high level of data protection. iDRAC6 employs the 128-bit SSL encryption standard. Supported cipher suites are listed in Appendix A. Ciphers supported by SSH are listed in Appendix B.

IPMI RMCP+ Encryption

iDRAC6 IPMI over LAN and SOL use RMCP+ for Authentication and Key exchange. For details on the RMCP+ protocol, see the IPMI 2.0 specification. iDRAC6 IPMI supports the following encryption algorithms:

- AES-CBC-128 (128-bit AES with CBC)
- RC4-128 (128-bit RC4)

SSL Certificate Management for Server iDRAC6 Authentication

IDRAC 6 ships with a default self-signed SSL certificate. iDRAC6 uses 1024-bit RSA with SHA-1 by default.

NOTE: Dell strongly recommends replacing the default certificate with your own SSL certificate to secure the IDRAC6 since systems ship with the same SSL certificate and with the same SSL private key.

The IDRAC 6 server SSL certificate is used by the web server, Virtual Media server, and Console

Redirection server. Administrators can replace the iDRAC6 server SSL certificate using the following steps:

- Generate the CSR and the Private Key from iDRAC6. 1024-bit, 2048-bit and 4096-bit RSAkey are supported.
  ***NOTE: Dell strongly recommends having CSR CN (common name) set to be the same as your iDRAC6 RAC name to avoid a host name mismatch complaint during SSL connection from browsers*.**
- Certificate asymmetric key size (RSA key size) can affect iDRAC 6 performance.
- Microsoft PKI best practices suggest using 1024-bit to secure your web server application.
- Sign the CSR by a trusted CA.
- Upload the signed CSR (Certificate) to iDRAC6.

Types of iDRAC6 Sessions

The level of security for the different interfaces to iDRAC6 is described in this section. All of these interfaces involve connecting to iDRAC6 remotely through a network connection except for the local RACADM command line interface.

Web Browser

The browser connects to the web server via the HTTPS port. Data streams are encrypted using 128-bit SSL to provide privacy and integrity. Any connection to the HTTP port will be redirected to HTTPS. Administrators can upload their own SSL certificate via an SSL CSR generation process to secure the web server. The default HTTP and HTTPS ports can be changed. iDRAC6 ensures that user access is restricted by user privileges.

Remote CLI

The Remote RACADM utility is a CLI tool that can be used to configure and manage a IDRAC 6. This scriptable utility can be installed on a management station. The RACADM installed on a management station is referred to as Remote RACADM. Remote RACADM communicates with IDRAC 6 through its network interface, and it uses an HTTPS channel to communicate with iDRAC6. A user must successfully pass his user authentication and must have sufficient privileges to be able to execute the desired command. Since Remote RACADM uses an HTTPS channel, all the command data and return data are encrypted by SSL. The encryption ciphers supported are the same as the web GUI interface.

Local CLI

The Local RACADM utility is a CLI tool that can be used to configure and manage iDRAC6 from the host server. This scriptable utility can only be installed on the managed system. The RACADM installed on a local managed system is called Local RACADM. Local RACADM communicates with iDRAC6 through its in-band IPMI host interface. Since it is installed on the local managed system, users are required to log in to the operating system to run this utility. The Local RACADM utility requires that a user must have a full administrator privilege or be a root user to use this utility. On a Microsoft Windows® system, a user must have the administrator privilege on the system to run the Local RACADM utility. If the user does not

have administrator privilege, an error message is displayed indicating that they do not have privileges. On a Linux-based system, a user must log in as root on the system to have a right to run the local RACADM utility. A user who can run Local RACADM is guaranteed to have administrator privilege to the system. The administrator privilege level indicates that the user has full rights to manage iDRAC6.

SSH

The SSH service is enabled by default on iDRAC6. RACADM CLI can be run in SSH. The SSH service can be disabled in the iDRAC6 configuration. iDRAC6 only supports SSH version 2 with DSA and the RSA host key algorithm. A unique 1024-bit DSA and 1024-bit RSA host key is generated during the first time power-up of iDRAC6 SSH.

SNMP

An SNMP agent runs on iDRAC6 by default. The iDRAC 6 SNMP agent is used by Dell OpenManage™ IT Assistant or other management frameworks to discover the IDRAC 6 out-of-band service point. The iDRAC6 only supports SNMP version 1. Since SNMP version 1 does not encrypt data and does not have a strong authentication protocol, there could be security concerns about the data leaking from IDRAC 6 (for example, service tag of a system or IP address of iDRAC6).

***NOTE: Dell strongly recommends using one of the following options to secure iDRAC6 from these concerns*:**

- If the IDRAC 6 SNMP agent is not being used in your environment, administrators can disable
- The IDRAC 6 SNMP service.
- Change the IDRAC 6 SNMP community name to secure their SNMP service. The default
- IDRAC 6 SNMP community name is “public.”
- Limit inbound SNMP access by only accepting specific client traffic by configuring the IDRAC 6
- Allowed client IP address range.

Virtual Media

Virtual media is a powerful remote access feature that allows a remote user to use a remote CD/floppy/image on the client side through the network. Administrators can use this feature for various administrative tasks such as remote operating system installation, remote diagnostics, remote driver/application software installation, and so on. A security authentication protocol is being used in the virtual media connection when a user logs into iDRAC6 web server via HTTPS with virtual media privilege and selects the virtual media tab. A request for a connection request command is sent to the iDRAC6 firmware. The iDRAC6 firmware responds by sending a set of virtual media configuration information along with an authentication key via the HTTPS (SSL encrypted) channel. The authentication key is randomly generated and is 32 bytes long. To prevent replay attacks, the authentication key is a one-time key and has its own limited lifetime. If a user selects an encrypted connection, the virtual media client software starts a connection via an SSL channel and sends the authentication key to the virtual media server for authentication. If the key passes the virtual media server authentication, a virtual media session will be established. Otherwise, a fail authentication message will be sent back to

the client and the connection will be dropped. All virtual media data is encrypted with AES256 and key exchanges via SSL, if an encrypted connection is selected. To keep virtual media operation going and still have session idle timeout security, iDRAC6 locks the web session when a virtual media operation is running and the web session is timed out. A user needs to re-authenticate to unlock the web session after session timeout. The virtual media operation will not be interrupted during the lock-out period.

Console Redirection

KVM login

Login credentials (username/password) are two random 32bit numbers, in ASCII string representation. They are not hashed. Credentials are used one time and have a configurable 60sec timeout. They are transmitted across an already secured channel (JNLP using a Web-GUI SSL connection).

Authentication and Encryption

IDRAC6 can continuously redirect the managed system's video, keyboard and mouse (KVM) to the management station via a proprietary compression algorithm. It is a very powerful feature, is very easy to use, and does not require any software installation on the managed system. A user can access this feature to remotely manage the system as if they were sitting in front of the system. A security authentication and encryption protocol has been implemented in console redirection to prevent a hostile, rogue client from breaking into the console redirect path without authenticating though the web server. 128-bit SSL encryption secures the keyboard keystrokes during the remote console redirection and therefore does not allow unauthorized "snooping" of the network traffic. The following sequence of security protocol operations is performed during the establishment of a console redirection session:

1. A user logs into the main web GUI then clicks the "Open Consoles" tab.
2. The Web GUI sends a pre-authentication request to the iDRAC6 web server via the HTTPS channel (SSL encrypted).
3. The iDRAC6 web server returns a set of secret data (including an encryption key) via the SSL channel. The console redirection authentication key (32 bytes long) is dynamically generated to prevent replay attack.
4. The Console redirection client sends a login command with an authentication key to a console redirection server keyboard/mouse port for authentication via SSL channel.
5. If authentication is successful, a console redirection session and two console redirection pipes (one for keyboard/mouse and one for video) are established. The keyboard/mouse pipe is always SSL encrypted. The video pipe encryption is optional. (Users can choose to encrypt or not to encrypt the video pipe before they start their console redirection session).

User Session Privacy

User session privacy is a security concern in the console redirection feature in iDRAC6. The following techniques are supported to maintain user session privacy and prevent user sessions from being hijacked:

- The default maximum number of console redirection sessions is limited to four. Administrators can configure the maximum number of console redirection sessions to one to avoid another remote user taking control of your console redirection session.

NOTE: Dell strongly recommends setting the maximum number of console redirection sessions to one if additional simultaneous remote access is not required.

- Remote users can use the Blank Local Video feature to prevent a local user from viewing the remote session.
  NOTE: Dell strongly recommends using the Blank Local Video feature if local access is not required during remote console redirection.
- Local users can use the Local RACADM CLI utility to disable console redirection when they log into the server and want to keep a session private. Users can re-enable console redirection after the remote session is over.
  NOTE: Dell strongly recommends disabling console redirection during local RACADM usage if simultaneous remote access is not required.

IPMI Out-of-Band Access Security

iDRAC6 implements IPMI version 2.0 which dramatically improved security over IPMI version 1.5. IPMI out-of-band including IPMI over LAN and SOL can be disabled if these features are not used in the user environment.
NOTE: Dell strongly recommends disabling the IPMI over LAN and SOL features if they are not required.

IPMI version 2.0 uses RMCP+ for authentication and encryption key exchange. The new algorithms provide a more robust key exchange process for establishing sessions and authenticating users. The IPMI message includes SOL payload carried over RMCP+ which can be encrypted. This option enables confidential remote configuration of parameters such as passwords and transfer of sensitive payload data over SOL. Please see the IPMI RMCP+ encryption section for all supported encryption algorithms. IPMI authorization and access to a system can be restricted through connection level, channel level privilege and user level privilege. Each channel, like IPMI LAN, can be limited to operate at one of three different privilege levels: user, operator or administrator. Similarly, each user can be created with any of these privileges for each channel. For example, when a particular channel is limited to operator level, only operator level operations can be performed on that channel. Refer to the IPMI version 2.0 specification for more details.

Other Security Features

VLAN

Virtual LAN tagging can be configured in the web browser interface. If enabled, the iDRAC6 firmware requires the presence of inserted fields in the network packets to send them through for processing. This provides a way to put multiple IP networks on the same switch in addition to being an extra measure of security.

Disabling Services and Changing the Service Port Number

There are several out-of-band services running on a IDRAC 6 by default. These services open a network port that listens for a connection.
NOTE: Dell strongly recommends disabling all unused services on iDRAC6 cards.

The following are services which can be enabled or disabled by administrators:

- SNMP Agent
- Telnet (disabled by default)
- SSH
- Web Server
- Console Redirection Service
- Virtual Media Service
- IPMI LAN interface (disabled by default)
- IPMI SOL interface

Ports must be correctly configured to allow iDRAC6 to work through firewalls. The following lists indicate the default ports used by iDRAC6:
22* SSH
23* Telnet
80* HTTP
443* HTTPS
623 RMCP/RMCP+
5900* Console Redirection keyboard/mouse, Virtual Media Service, Virtual Media Secure Service, Console Redirection video
* Configurable port

iDRAC6 Client Ports…

25 SMTP
53 DNS
68 DHCP-assigned IP address
69 TFTP
162 SNMP trap
636 LDAPS
3269 LDAPS for global catalog (GC)

Firewall

To prevent unauthorized access to the remote system, IDRAC 6 provides the following features:

- IP address filtering (IPRange) — defines a specific range of IP addresses that can access the iDRAC 6
- IP address blocking — limits the number of failed login attempts from a specific IP address

IP Blocking

This feature is disabled in the IDRAC 6 default configuration. Use the RACADM config subcommand or the Web-based interface to enable this feature.

Additionally, use this feature in conjunction with the appropriate session idle timeout values and defined security plan for your network.

IP Filtering (IPRange) and IP address filtering (or IP Range Checking) allows iDRAC6 to be accessed only from clients or management workstations whose IP addresses are within a user specific range. All other logins are denied.

Invalid Login Attack Blocking

To prevent a repeat attack and a password guess attack to your remote system, the IDRAC 6 provides IP address blocking. This feature limits the number of failed login attempts from a specific IP address.

The IP blocking feature dynamically determines when excessive login failures have occurred from a specific IP address and blocks (or prevents) the IP address from logging into the IDRAC 6 for the time span configured in the IDRAC 6.

As login failures accumulate from a specific IP address, they are "aged" by an internal counter. When the login failures reach the maximum age of the internal counter window, they are deleted (or forgiven). When a valid login occurs from an IP address that is not penalized (the excessive login failures are being held in cfgRacTuneIpBlkPenaltyTime), all previous login failures for the IP address are deleted. The failure history cannot be cleared except by a valid login attempt. When the excessive failures are detected, login will be blocked for a pre-selected time span. However, this feature can be disabled to allow login from the targeted IP address.

NOTE: Dell strongly recommends using the IP blocking feature and setting the limit on invalid login attempts to your environment requirements.

Event Logging

The iDRAC Log can be viewed in the browser interface or retrieved using the RACADM CLI. It will show open and closed sessions with timestamps. It will also show failed login attempts to create an audit trail of evidence if there ever was a breach.

Recommended Practices

Dell recommends the following practices to enhance security with iDRAC6.

Use a dedicated NIC for the iDRAC. This isolates the management processor on its own network as discussed above. Further, access rights can be given only to a select few individual administrators.

Change or disable the default local user account. This is a relatively well known default credential.

Implement advanced user authentication measures such as TFA and directory services. This way user databases can be controlled from a central point. Additionally, TFA offers an additional measure of security.

Restrict privileges, especially to remote desktop (vKVM). Although traffic is encrypted and uses a proprietary compression algorithm, any possible access to the host process should be limited.

Disable ports not in use.

Use a custom PKI (Private Key Infrastructure). Upload a private key and a certificate to the iDRAC6 to overwrite the default certificate that is shipped with the units to ensure secure iDRAC6 authentication.

Acronyms

Term	Definition
AD	Active Directory
CA	Certificate Authorization
CAST 128	CAST Algorithm 128-bit
CD	Compact Disk
CLI	Command Line Interface
CSR	Certificate Signing Request
3 DES	Triple Data Encryption Standard
DH	Diffie-Hellman
DNS	Domain Name Server
iDRAC	Integrated Dell Remote Access Controller
DSA	Digital Signature Algorithm
GUI	Graphical User Interface
TFA	Two Factor Authentication
vKVM	Virtual Keyboard, Video, Mouse

Further information

Information and papers about the Lifecycle Controller and Dell's embedded management solution including iDRAC6 can be found at the following link:
http://www.delltechcenter.com/page/Lifecycle+Controller

More information can be found in the iDRAC6 user's guides at this link:
http://support.dell.com/support/edocs/software/smdrac3/idrac/index.htm

The Kerberos Network Authentication Service:
http://tools.ietf.org/html/rfc4120

Appendix A: Supported SSL Cipher Suites

IDRAC 6 supports SSL version 3 and TLS version 1.0. SSL connections are established after negotiating a matching cipher suite with the browser out of this list in this order:

- DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
- DHE-DSS-AES256-SHA SSLv3 Kx=DH Au=DSS Enc=AES(256) Mac=SHA1
- AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
- EDH-RSA-DES-CBC3-SHA SSLv3 Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
- EDH-DSS-DES-CBC3-SHA SSLv3 Kx=DH Au=DSS Enc=3DES(168) Mac=SHA1
- DES-CBC3-SHA SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
- DES-CBC3-MD5 SSLv2 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5
- DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
- DHE-DSS-AES128-SHA SSLv3 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1
- AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
- IDEA-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=IDEA(128) Mac=SHA1
- IDEA-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=IDEA(128) Mac=MD5
- RC2-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
- RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
- RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
- RC4-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
- EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH Au=RSA Enc=DES(56) Mac=SHA1
- EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH Au=DSS Enc=DES(56) Mac=SHA1
- DES-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1
- DES-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5
- EXP-EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export
- EXP-EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH(512) Au=DSS Enc=DES(40) Mac=SHA1 export
- EXP-DES-CBC-SHA SSLv3 Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
- EXP-RC2-CBC-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
- EXP-RC2-CBC-MD5 SSLv2 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
- EXP-RC4-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
- EXP-RC4-MD5 SSLv2 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

Appendix B: Secure Shell Encryption

IDRAC 6 supports only SSH-2.0 because SSH-1.0 is not considered secure.
The following are ciphers supported by the IDRAC 6 SSH:

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr
- arcfour
- blowfish-cbc
- cast128-cbc