DRAC 4
Dell Remote Access Controller 4 Security

Dell | Enterprise Systems

Table of Contents

Terminology

Term	Definition
3 DES	Triple Data Encryption Standard
ADS	Active Directory Services
CA	Certificate Authorization
CAST 128	CAST Algorithm 128 bit
CD	Compact Disk
CLI	Command Line Interface
CN	Common Name
CSR	Certificate Signing Request
DH	Diffie-hellman
DNS	Domain Name Server
DRAC 4	Dell Remote Access Controller 4
DSA	Digital Signature Algorithm
GUI	Graphic User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
KVM	Keyboard Video Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol Secure
LOM	Lay on Mother Board
MAC	Media Access Control
MD5	Message Digest Algorithm Number 5
MS	Microsoft
NIC	Network Interface Card
NVRAM	Non Volatile Random Access Memory
OS	Operating System
PET	Platform Event Trap
PKI	Public Key Infrastructure
RAC	Remote Access Controller
RC4	ARC Four Algorithm
RMCP	Remote Management Control Protocol
RSA	Rivest Shamir Adleman

Term	Definition
SEL	System EvenT Log
SHA1	Seane Hash Algorithm
SMCLP	Server Management Command Line Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOL	Serial Over Lan
SSH	Secured Shell
SSL	Secured Socket Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TLS1.0	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VMCLI	Virtual Machine Command Line Interface
VNC	Virtual Network Computing

Introduction

Today, managing distributed servers from a remote location is a critical requirement.

DRAC 4 enables users to remotely monitor, troubleshoot and repair servers, even when the server operating system is down. DRAC 4 offers a rich set of features such as virtual media, virtual KVM which can make the system less prone to security risks. DRAC 4 security features mitigate the security risks that exist while data is being transmitted across the network. This white paper briefly describes the security features that DRAC 4 uses to help ensure authentication, authorization, privacy and data integrity.

Authentication and Authorization

Login Using Local Account

The DRAC 4 comes with a default local user account pre-configured with an administrator role. The default user name for this account is “root” and the default password is “calvin”.

Note: Dell strongly recommends changing the default user name and password settings during deployment of the DRAC 4.

DRAC 4 supports up to 16 local users. Each user can be enabled or disabled. You can secure the DRAC 4 by disabling all local user accounts and using only Microsoft® Active Directory® users since MS Active Directory is considered to have stronger secure policy management.

Local users’ username and password can be changed. DRAC 4 local users’ account policy is as following:

- Anonymous user is NOT supported
- NULL user name is NOT supported
- NULL password is NOT supported
- Maximum user name length is 16 characters
- Maximum user password length is 20 characters

The DRAC 4 local user password is stored as an MD5 hashing value on its NVRAM.

DRAC 4 supports privileged-based access to a DRAC 4. Every DRAC 4 local user or MS Active Directory user has a privilege associate with it. The privilege is per channel per user. The privilege defines the kind of rights a user has on the DRAC 4.

The DRAC 4 offers nine privileges. Each user can have any combination of the nine privileges. The nine privileges are as follows:

RAC Login User Privilege

This privilege allows a user to log in to the DRAC 4 card. An administrator can easily disable a user from a DRAC 4 by removing this privilege. Removing the login privilege from a user is not the same as deleting a user. The user will remain in the user database but will not be able to log in and use this DRAC 4 card. An administrator can quickly re-enable the user by granting the log in privilege without totally reconfiguring the user settings.

RAC Card Configuration Privilege

This privilege allows a user to change all DRAC 4 card configurations except for the user configuration (for example, out-of-band NIC configuration, SNMP trap configuration, SSL certificate configuration, and so on).

RAC User Configuration Privilege

This privilege allows a user to add or delete a user or change existing user privileges.

RAC Log Clear Privilege

This privilege allows a user to clear the SEL, RAC log, or last crash screen log.

RAC Server Reset and Power-On/Off Privilege

This privilege allows a user to do any power management operation (like reset or power-on/off a system).

RAC Console Redirection Privilege

This privilege allows a user to use the console redirection feature.

RAC Virtual Media Privilege

This privilege allows a user to use the virtual media feature.

RAC Test Alert Privilege

This privilege allows a user to submit a request to the DRAC 4 to test an SNMP trap alert to a pre-configured destination.

RAC Debug Command Privilege

This privilege allows a user to issue any debug command. Most debug commands are used to help debug or diagnose a DRAC 4.

Note: Dell strongly recommends assigning this privilege only to administrators or service personnel required to help debug or diagnose the DRAC 4.

Login Using Active Directory with Dell Schema Extension

A directory service maintains a common database of all information needed for controlling users, computers, printers, and so forth on a network. If your company uses the Active Directory service software, you can configure the software to provide access to the DRAC 4. This access allows you to add and control DRAC 4 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 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.

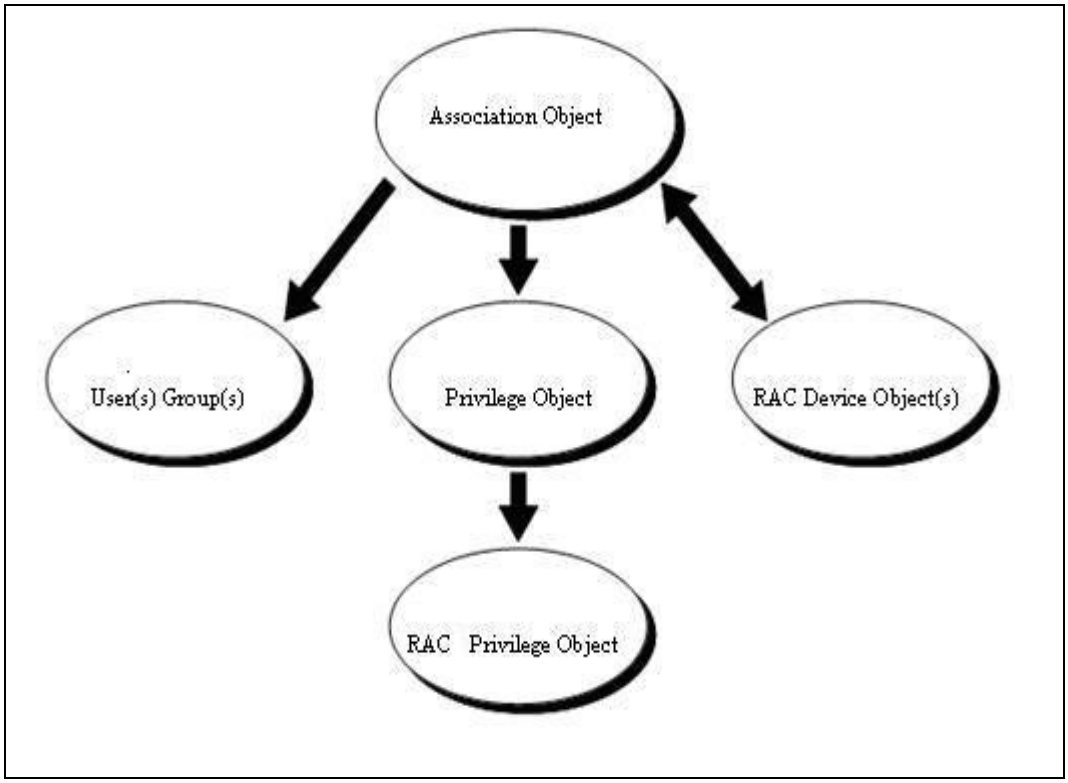

Figure 1: Dell Extended Schema Active Directory Architecture

DRAC 4 authenticates against Active Directory using LDAP simple binding and queries Active Directory objects using an SSL channel. All data (including user name and password) for authentication are sent using an encrypted channel to Active Directory. When a DRAC 4 establishes an SSL connection with Active Directory Domain Controller, it verifies the Domain Controller entity using SSL server authentication. The root CA SSL certificate (which is used to sign all the Domain Controller SSL certificates) has been imported to the DRAC 4. DRAC 4 supports up to a 4096-bit root CA certificate and Domain Controller SSL certificate.

Note: Dell strongly recommends following the Microsoft PKI (Public Key Infrastructure) 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 a DRAC 4, the 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 a DRAC 4 has to be added to the Dell Association object. The RAC device object name has to be configured to the DRAC 4.

The basis for searching Active Directory to authenticate and authorize the RAC user is that there is a member-memberOf relationship with the Association object. It is derived from the group. Every member of a group has a corresponding Linked attribute member called memberOf that is part of the User class.

To authenticate a user with LDAP, obtain the memberOf attribute that contains all the groups the user is a member of. Of these groups, locate the ones that have the dellAssociationObject class.

Note: The user can be a member of multiple Association object classes.

When the dellAssociationObject class that the user is a member of is found, look for the dellProductMembers attribute. Look at this attribute to determine if the RacDevice being authenticated is part of the attribute.

Note: dellProductMembers can be groups of RACs and will retain the member-memberOf relationship.

Look at the list using the Member attribute for all of the groups that are in the list. If the name of the RAC device that is being authenticated is in the list, the user has been authenticated.

Read the dellPrivilegeObject attributes and enter them to the RAC as the authorization data (Privileges).

Login Using Active Directory without Dell Schema Extension

Note: Requires DRAC 4 version 1.50 firmware and later.

Dell has been using Active Directory to manage DRAC 4 users and their access privileges on different DRAC 4 cards. 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 now provides a standard schema solution in addition to the schema extension. This solution provides the same flexibility of the current schema-extending solution. It allows granting different users different privileges on different DRAC 4 cards. 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 the Active Directory 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 DRAC 4 cards. The privilege of that role group has been defined in each individual DRAC 4 configuration database. Different DRAC 4 cards can give the same role group object different privileges.

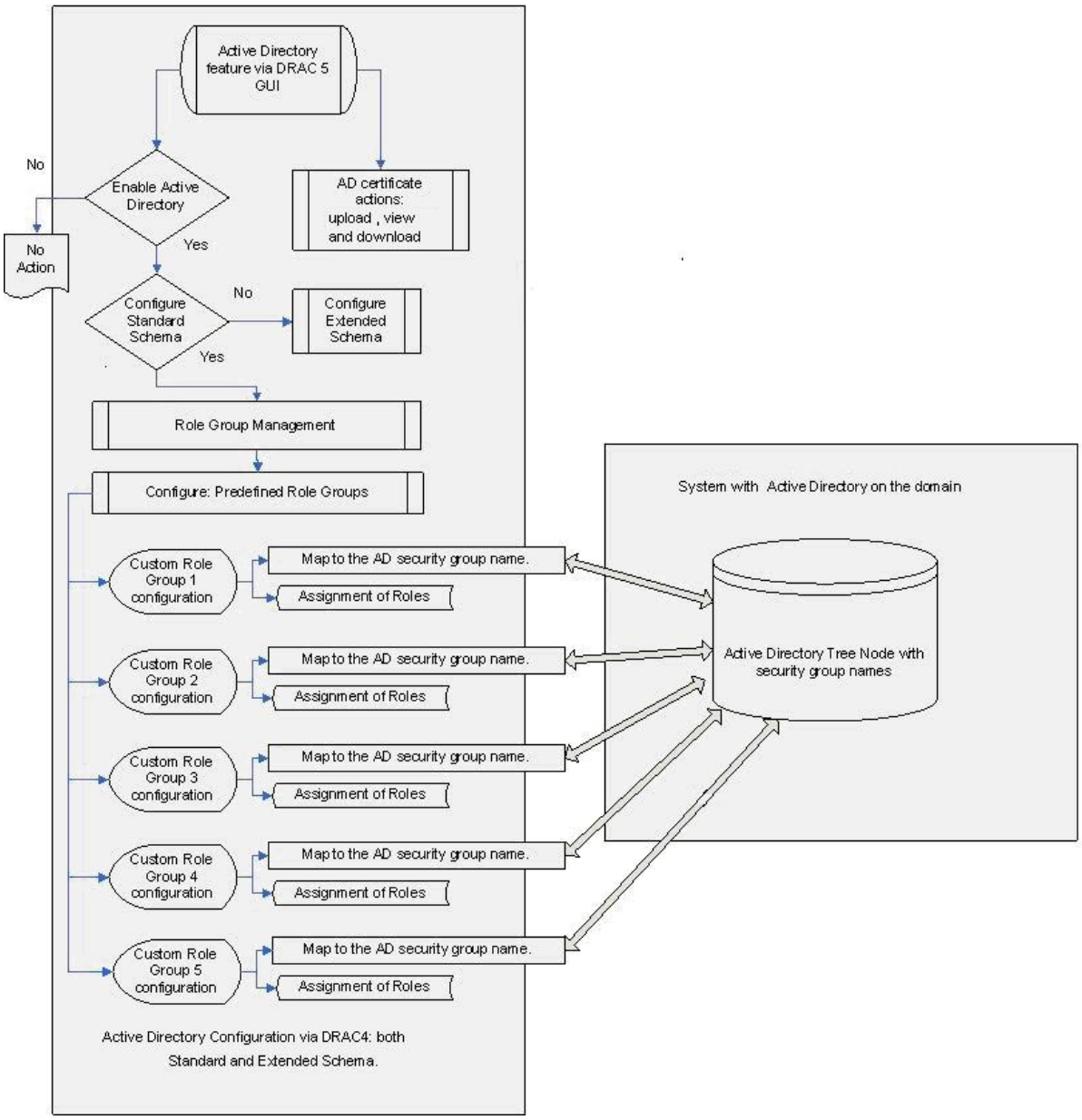

Figure 2: Dell Standard Schema Active Directory Architecture

Encryption

The SSL security protocol that is built upon public key/private key encryption technology has been universally accepted on the World Wide Web for authenticated and encrypted communication between clients and servers to prevent eavesdropping across the network. Running above TCP/IP and below higher-level protocols (such as HTTP), SSL allows an SSL-enabled server to authenticate itself to an SSL-enabled client and the client to authenticate itself to the server. SSL allows both servers to establish an encrypted connection.

SSL Certificate Management

DRAC 4 ships with a default self-signed SSL certificate. It uses a 1024-bit RSA with MD5.

Note: Dell strongly recommends replacing the default certificate with your own SSL certificate to secure the DRAC 4 since all DRAC 4 cards ship with the same SSL certificate and with the same SSL private key.

The DRAC 4 server SSL certificate is used by the web server and remote RACADM CLI.

Administrators can replace DRAC 4 server SSL certificate using the following steps:

1) Generate the CSR and Private Key from a DRAC 4. A 1024-bit RSA key is supported.

Note: Dell strongly recommends having CSR CN (common name) set to be the same as your DRAC 4 RAC name to avoid a host name mismatch complaint during SSL connection from browsers.

2) Sign the CSR by a trusted CA.

3) Upload the signed CSR to the DRAC 4.

Supported SSL Cipher Suites

DRAC 4 supports SSLv3 and TLS1.0.

The following are Ciphers supported on DRAC 4:

- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA

Secure Shell Encryption

DRAC 4 supports only SSH-2.0 because SSH-1.0 is not considered secure.

The following are ciphers supported by the DRAC 4 SSH:

- Public key: DSA
- Hash: SHA-1, MD5
- Symmetric: 3DES, RC4, AES-128, AES-192, AES-256

Event Logging

DRAC 4 has a persistent log that stores all critical events like user login/logout, DRAC 4 configuration changes, critical operations to a server via DRAC 4, and so on. Administrators can use this log to audit critical operations on the DRAC 4.

Log Format

All log entries include:

- Time of the event
- Application associated with the event
- User or initiating process
- Remote IP address associated with the event
- Detailed description of the event

Log Events

The following are categories of events logged in the DRAC 4 log:

- All valid and failed login attempts
- All logout events
- Log Cleared
- All PET alerts or test alerts sent by a DRAC 4
- All server power management used by a DRAC 4 (such as power on, power off, power cycle, and hard reset to a system)
- DRAC firmware update
- Start /Stop a DRAC 4 Virtual Media session
- Start/Stop a DRAC 4 Console Redirection session
- Access to DRAC 4

Disabling Services and Changing Service Port Number

There are several out-of-band services running on a DRAC 4 by default. These services open a network port that listens for a connection.

Note: Dell strongly recommends disabling all unused services on DRAC 4 cards.

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

- SNMP Agent
- Telnet (disabled by default)
- SSH
- Remote RACADM

Ports must be correctly configured to allow DRAC 4 to work through firewalls. Table 1 lists the ports used by DRAC 4.

Port #	Protocol	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
22	SSHv2	TCP	1.30	128 bit	In/Out	Optional SSH CLI management	Yes
23	Telnet	TCP	1.0	None	In/Out	Optional Telnet CLI management	Yes
25	SMTP	TCP	1.0	None	In/Out	Optional e-mail alert messages	No
53	DNS	UDP	1.20	None	In/Out	Dynamic DNS registration of the host name assigned within DRAC	No
68	DHCP	UDP	1.0	None	In/Out	DHCP assigned IP address	No
69	TFTP	UDP	1.0	None	In/Out	Firmware update by Trivial FTP	No
80	HTTP	TCP	1.0	None	In/Out	Web GUI redirected to HTTPS	Yes
161	SNMP	UDP	1.0	None	In/Out	SNMP query management	No
162	SNMP	UDP	1.0	None	Out	SNMP trap event	No
443	HTTPS	TCP	1.0	128-bit SSL	In/Out	Web management GUI and remote RACADM CLI utility	Yes
636	LDAPS	TCP	1.0	128-bit SSL	In/Out	Optional ADS	No

Port #	Protocol	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
						authentication	
3269	LDAPS	TCP	1.0	128-bit SSL	In/Out	Optional ADS authentication	No
3668	Proprietary	TCP	1.0	None	In/Out	CD/diskette virtual media service	Yes
5869	Proprietary	TCP	1.0	None	In/Out	Remote RACADM	No
5900	Proprietary	TCP	1.0	128-bit RC4, Keyboard/mouse traffic only	In/Out	Video redirection	Yes

Table 1: Port Configuration for DRAC 4

Web Browser Security

The browser connects to your web server using the HTTPS port. All the data streams are encrypted using 128-bit SSL to provide privacy and integrity. Any connection to the HTTP port is redirected to HTTPS. Administrators can upload their own SSL certificate using an SSL CSR generation process to secure the web server. The default HTTP and HTTPS ports can be changed. DRAC 4 is designed to ensure that user access is restricted by user privileges.

Remote CLI Security

The Remote RACADM utility is a CLI tool that can be used to configure and manage a DRAC 4. This scriptable utility can be installed on a management station. The RACADM installed on a management station is referred to as Remote RACADM. The Remote RACADM communicates with DRAC 4 through its network interface and uses an HTTPS channel to communicate with DRAC 4. A user must successfully pass its 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 Security

The Local RACADM utility is a CLI tool that can be used to configure and manage a DRAC 4 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 DRAC 4 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 administrator privileges on the system to run the Local RACADM utility. If the user does not have administrator privileges, an error message is displayed indicating that they do not have privileges to run this utility. 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 DRAC 4 including configuration, power management, firmware update, debug, and so on.

SSH Security

The SSH service is enabled by default on DRAC 4. The RACADM CLI can be run in SSH. The SSH service can be disabled using DRAC 4 configuration setting. DRAC 4 only supports SSH version 2.

DRAC 4 supports DSA and RSA host key algorithms. A unique 1024-bit DSA and 1024-bit RSA host key is generated during a DRAC 4 the first time that power is turned on.

DRAC 4 SSH supports:

- The SHA-1 and MD5 hash algorithm
- The Diffie-hellman-group1-sha1 key exchange algorithm
- The DSA public key (asymmetric encryption) algorithm
- 3DES-CBC, RC4, AES-128, AES-192, AES-256 symmetric encryption

DRAC 4 SSH only supports password user authentication.

SNMP Security

An SNMP agent runs on a DRAC 4 by default. The DRAC 4 SNMP agent is used by Dell OpenManage™ IT Assistant or other management frameworks to discover the DRAC 4 out-of-band service point such as a web GUI URL. DRAC 4 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 DRAC 4 (for example, service tag of a system or IP address of DRAC 4, and so on).

Note: Dell strongly recommends using one of the following options to secure the DRAC 4 card from these concerns:

- If the DRAC 4 SNMP agent is not being used in your environment, administrators can disable the DRAC 4 SNMP service.
- Change the DRAC 4 SNMP community name to secure their SNMP service. The default DRAC 4 SNMP community name is “public.”

Virtual Media Security

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 a DRAC 4 web server using HTTPS with virtual media privilege and selects the virtual media tab or uses the VMCLI utility. A request for a connection request command is sent to the DRAC 4 firmware. The DRAC 4 firmware responds by sending a set of virtual media configuration information along with an authentication key using the HTTPS (SSL encrypted) channel. The authentication key is randomly generated and is 16 bytes long. To prevent replay attacks, the authentication key is a one-time key and has its own limited lifetime. If it passes the virtual media server authentication, a virtual media session is established. If it does not pass, an authentication failure message is sent back to a client and the connection is dropped.

To keep the virtual media operation going and still have session idle timeout security, DRAC 4 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.

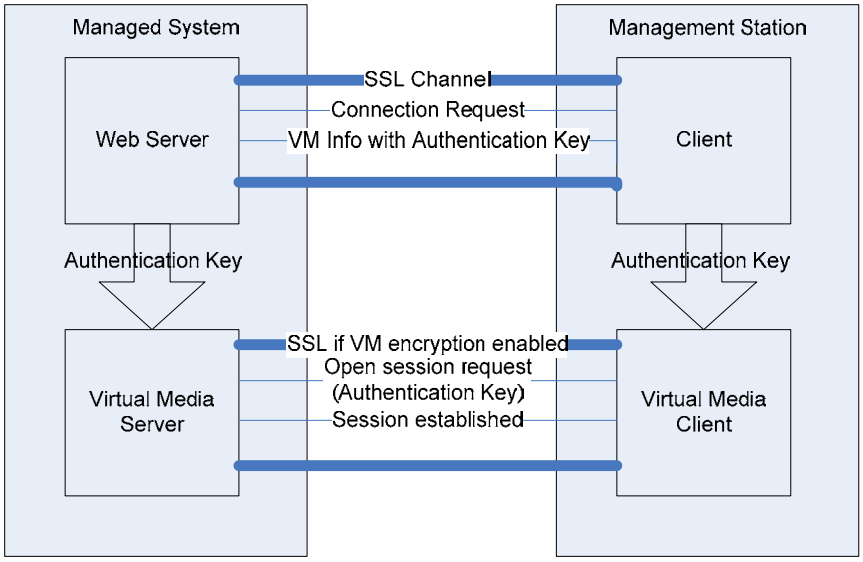

Figure 3: Virtual Media Architecture

Console Redirection Security

Authentication and Encryption

DRAC 4 can continuously redirect the managed system's KVM to the management station. 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.

A security authentication and encryption protocol has been implemented in console redirection to help prevent a hostile, rogue client from breaking into the console redirect path without authenticating though the web server. 128-bit RC4 encryption secures the keyboard keystrokes during the remote console redirection and therefore does not allow unauthorized "snooping" of the network traffic.

When a user logs into the main web GUI and clicks the **Open Consoles** tab, the following security protocol operations occur:

- The web GUI sends a pre-authentication request to the DRAC 4 web server through the HTTPS channel (SSL encrypted).
- The DRAC 4 web server returns a set of secret data (including authentication and encryption keys) using the SSL channel. The console redirection authentication key (16 bytes long) is dynamically generated to prevent replay attack.
- The console redirection client sends a login command with an authentication key to a console redirection server for authentication.
- 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 128-bit RC4 encrypted. The video pipe encryption is optional.

Note: Users can choose to encrypt or not to encrypt the video pipe before they start their console redirection session.

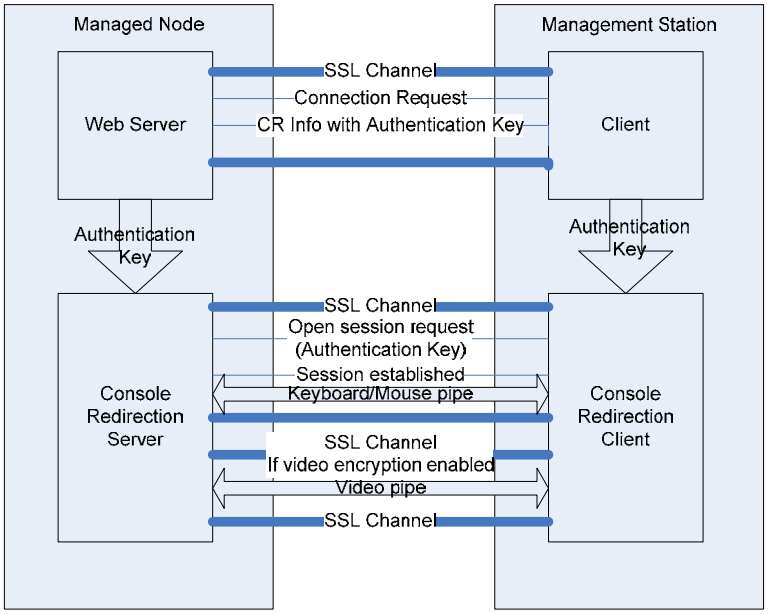

Figure 4: Console Redirection Architecture

User Session Privacy

User session privacy is a security concern in the console redirection feature in DRAC 4.

DRAC 4 supports the following techniques to maintain user session privacy and prevent user sessions from being hijacked:

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

In addition to DRAC 4 console redirection, users can use Remote Desktop on the Windows operating system and VNC console redirection on a Linux-based operating system to perform post-operating system console redirection. For additional information, refer to the Remote Desktop or VNC console redirection documentation.