DRAC 5
Dell Remote Access Card 5 Security

Table of Contents

Terminology

Term	Definition
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
DRAC 5	Dell Remote Access Controller
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
SEL	System Event Log

Term	Definition
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
VNC	Virtual Network Computing

Introduction

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

DRAC 5 enables users to remotely monitor, troubleshoot, and repair servers even when the server is down. DRAC 5 offers a rich set of features like virtual media, virtual KVM, and so on, which have the potential to make the system prone to security risks. DRAC 5 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 5 uses to help ensure authentication, authorization, privacy, and data integrity.

Authentication and Authorization

Log in via Local Account

The DRAC 5 ships with a default local user account that is pre-configured with an administrator role. This default user name is "root" and the password is "calvin" for this user.

Dell strongly recommends changing this default setting during deployment of the DRAC 5.

DRAC 5 supports up to 16 local users. Each user can be enabled or disabled. You can secure the DRAC 5 by disabling all local user accounts and using only Microsoft® Active Directory® users since Active Directory is considered to have stronger secure policy management.

Local users' user names and passwords can be changed. DRAC 5 local users' account policy is as follows:

- 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

DRAC 5 local user account information is stored on NVRAM and is encrypted via a proprietary algorithm.

DRAC 5 supports privilege-based access to a DRAC. Every local user or Active Directory user has a privilege set associated with it. The privilege is per channel per user. The privilege set decides what kind of rights a user has on the DRAC 5 on each of the access channels.

There are three types of access channels on DRAC 5:

- IPMI LAN channel
- IPMI Serial channel
- RAC channel – including RAC web GUI, RAC serial/telnet/SSH console, RACADM CLI, RAC SM-CLP, RAC virtual media, RAC console redirection

IPMI LAN and IPMI serial channel privilege are defined in the IPMI 2.0 specification. (See IPMI Out-of-band Access Security for further information.)

The DRAC 5 RAC channel has 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 5 card. An administrator can easily disable a user from a DRAC 5 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 5 card. An administrator can quickly re-enable this user by granting the login privilege without having to totally reconfigure this user.

RAC Card Configuration Privilege

This privilege allows a user to change all DRAC 5 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 System Event Log (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 DRAC 5 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 of debug commands are used to help debug or diagnose a DRAC 5.

Dell strongly recommends assigning this privilege only to administrators or service personnel required to help debug or diagnose the DRAC 5.

Log in via 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 5 allowing you to add and control DRAC 5 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.

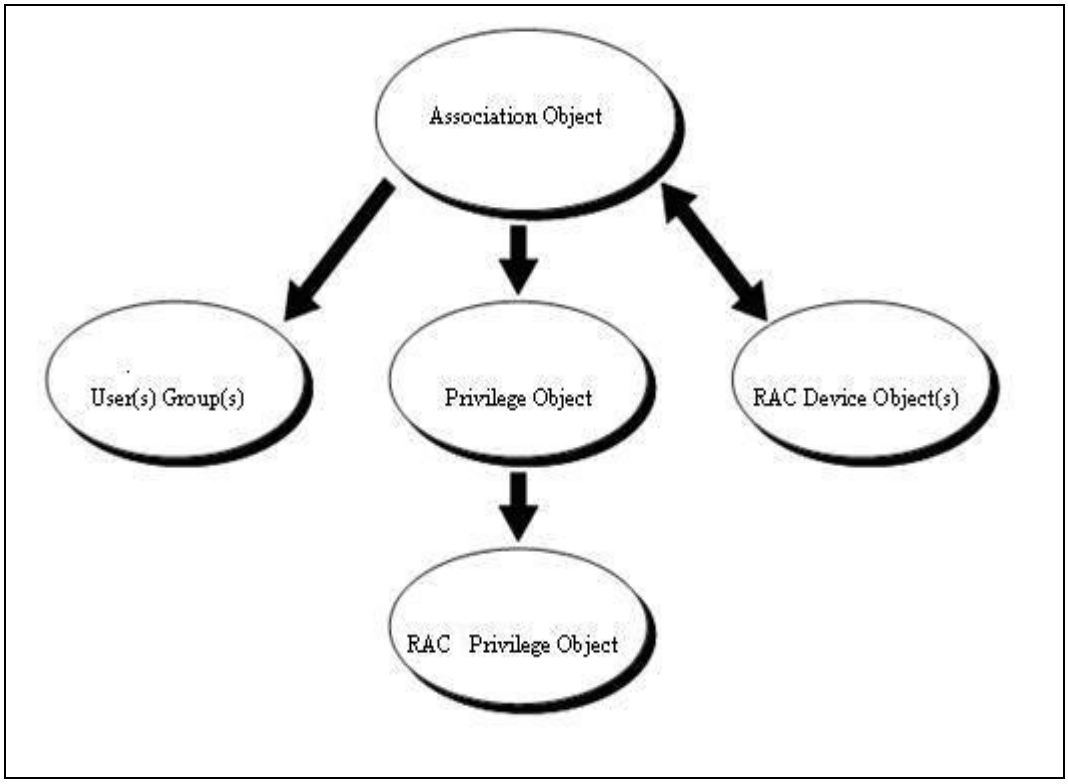

Figure 1: Dell Extended Schema Active Directory Architecture

DRAC 5 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 a DRAC 5 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 DRAC. DRAC 5 supports up to a 4096-bit root CA certificate and Domain Controller SSL certificate.

Dell strongly recommend 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 a DRAC 5, 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 a DRAC 5 is added to Dell Association object. The RAC device object name has to be configured to that DRAC 5.

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 -- it is derived from group. 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. 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).

Log in via Active Directory Without Dell Schema Extension

NOTE: Requires DRAC 5 version 1.20 firmware and later.

Dell has been using Active Directory to manage DRAC 5 users and their access privileges on different DRAC 5 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 will provide the same flexibility of the current schema-extending solution – it will allow granting different users different privileges on different DRAC 5 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 5 cards. The privilege of that role group has been defined in each individual DRAC 5 configuration database. Different DRAC 5 cards can give the same role group object different privileges.

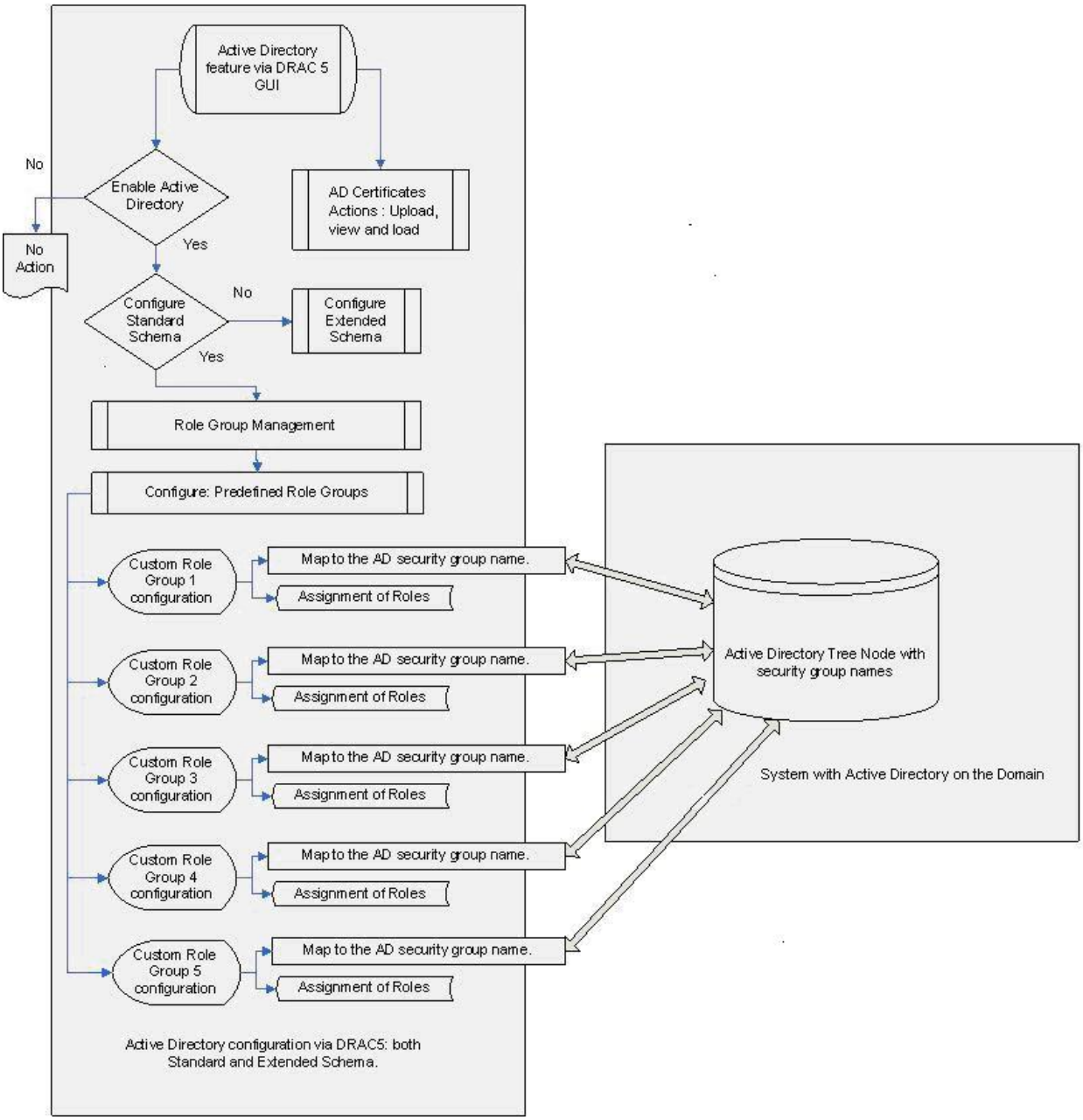

Figure 2: Dell Standard Schema Active Directory Architecture

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 5 ships with a default self-signed SSL certificate. DRAC 5 uses 1024-bit RSA with SHA-1.

Dell strongly recommends replacing the default certificate with your own SSL certificate to secure the DRAC 5 since all DRAC 5 cards ship with the same SSL certificate and with the same SSL private key.

The DRAC 5 server SSL certificate is used by the web server, Virtual Media server, and Console Redirection server.

Administrators can replace the DRAC 5 server SSL certificate using the following steps:

- Generate the CSR and the Private Key from a DRAC 5. 1024-bit, 2048-bit and 4096-bit RSA key are supported.

Dell strongly recommends having CSR CN (common name) set to be the same as your DRAC 5 RAC name to avoid a host name mismatch complaint during SSL connection from browsers.

- Large certificate asymmetric key size (RSA key size) can affect DRAC 5 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 your DRAC 5.

Supported SSL Cipher Suites

DRAC 5 supports SSL version 3 and TLS version 1.0. The following are ciphers supported on DRAC 5:

- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_MD5
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

Secure Shell Encryption

DRAC 5 supports only SSH-2.0 because SSH-1.0 is not considered secure.

The following are ciphers supported by the DRAC 5 SSH:

- **Public key: DSA, RSA**
- **Hash: SHA-1, MD5**
- **Symmetric: 3DES, RC4, Blowfish, CAST-128**

IPMI RMCP+ Encryption

DRAC 5 IPMI over LAN and SOL use RMCP+ for Authentication and Key exchange. For details on the RMCP+ protocol, see the IPMI 2.0 specification.

DRAC 5 IPMI supports the following encryption algorithms:

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

Event Logging

DRAC 5 has a persistent log which stores all critical events like user login/logout, DRAC 5 configuration changes, and critical operations to a server via DRAC 5, and so on. Administrators can use this log to audit critical operations on the DRAC 5.

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 5 log:

- All valid and failed login attempts
- All logout events
- All security policy changes, like channel privilege, IP blocking, and so on
- All user account management changes (such as user creation or deletion, user privilege changes, and so on)
- All PET alerts or test alerts sent by a DRAC 5
- All server power management via a DRAC 5 such as power on, power off, power cycle, and hard reset to a system
- DRAC 5 firmware update
- Start /Stop a DRAC 5 Virtual Media session
- Start/Stop a DRAC 5 Console Redirection session

Disabling Services and Changing the Service Port Number

There are several out-of-band services running on a DRAC 5 by default. These services open a network port that listens for a connection.

Dell strongly recommends disabling all unused services on DRAC 5 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 DRAC 5 to work through firewalls. The following table lists the ports used by DRAC 5.

Port #	Protocol	Port Type	DRAC 5 Firmware Version	Maximum Encryption Level	Direction	Usage	Configurable
22	SSH version 2	TCP	1.0	128-bit	In/Out	Optional Secure Shell (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	1.0	None	In/Out	Dynamic Domain name server (DNS) registration of the host name assigned within DRAC 5 and ADS authentication DNS lookup	No

Port #	Protocol	Port Type	DRAC 5 Firmware Version	Maximum Encryption Level	Direction	Usage	Configurable
68	DHCP	UDP	1.0	None	In/Out	DHCP assigned IP address	No
69	TFTP	UDP	1.0	None	In/Out	Firmware update via 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
623	RMCP/RMCP+	UDP	1.0	128-bit RC4 or AES	In/Out	IPMI Over LAN and IPMI SOL	No
636	LDAPS	TCP	1.0	128-bit SSL	In/Out	Optional Active Directory Services (ADS) authentication	No
3269	LDAPS	TCP	1.0	128-bit SSL	In/Out	Optional Active Directory Services (ADS) authentication	No
3668	Proprietary	TCP	1.0	None	In/Out	CD/diskette virtual media service	Yes
3669	Proprietary	TCP	1.0	128-bit SSL	In/Out	CD/diskette virtual media service	Yes
5900	Proprietary	TCP	1.0	128-bit SSL	In/Out	Video redirection	Yes
5901	Proprietary	TCP	1.0	128-bit SSL	In/Out	Keyboard/Mouse redirection	Yes

Table 1: Port Configuration for DRAC 5

Security Policy

To prevent unauthorized access to the remote system, DRAC 5 provides the following features which have been described in ”IP Blocking” and “Invalid Login Attack Blocking.”

- IP address filtering (IPRange) — defines a specific range of IP addresses that can access the DRAC 5
- IP address blocking — limits the number of failed login attempts from a specific IP address

IP Blocking

This feature is disabled in the DRAC 5 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 a defined security plan for your network.

IP Filtering (IPRange) and IP address filtering (or IP Range Checking) allow DRAC 5 to be accessed only from clients or management workstations whose IP addresses are within a user-specific range. All other logins are denied.

IP filtering compares the IP address of an incoming login to the IP address range that is specified by the following properties:

Property	Description
cfgRacTuneIPRangeEnable	Enables the IP range checking feature.
cfgRacTuneIPRangeAddr	Determines the acceptable IP address bit pattern positions depending on the 1’s in the subnet mask. This property is bitwise, and uses the “width with cfgRacTuneIPRangeMask” property to determine the upper portion of the allowed IP address. Any IP address that contains this bit pattern in its upper bits is allowed to establish a DRAC 5 session. Logins from IP addresses that are outside this range will fail. The default values in each property allow an address range from 192.168.1.0 to 192.168.1.255 to establish a DRAC 5 session.
cfgRacTuneIPRangeMask	Defines the significant bit positions in the IP address. The subnet mask should be in the form of a netmask, where the more significant bits are all 1’s with a single transition to all zeros in the lower-order bits.

Table 2: Properties for RAC Tuning

Invalid Login Attack Blocking

To prevent a repeat attack and a password guess attack to your remote system, the DRAC 5 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 DRAC 5 for the time span configured in the DRAC 5.

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.

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

Shared NIC Security

The DRAC 5 on 9*xxx* Generation Dell servers has the capability to use the host LOM for DRAC 5 management traffic instead of a dedicated NIC. In this case, the host LOM shares the host traffic with DRAC 5 management traffic.

This feature has an advantage for customers who do not want to maintain a separate network for management traffic. It can reduce the cabling mess and network switch port requirements. The shared NIC (LOM) contains two separate MAC addresses – one for the DRAC 5 traffic and another for the host system traffic. The MAC layer is a sub-layer in the hardware data-link layer. DRAC 5 maintains its own IP address, which ensures that a client can address DRAC 5 independently of the host system even though the host and management traffic share the same port.

The following figure describes the shared NIC architecture in DRAC 5 hardware.

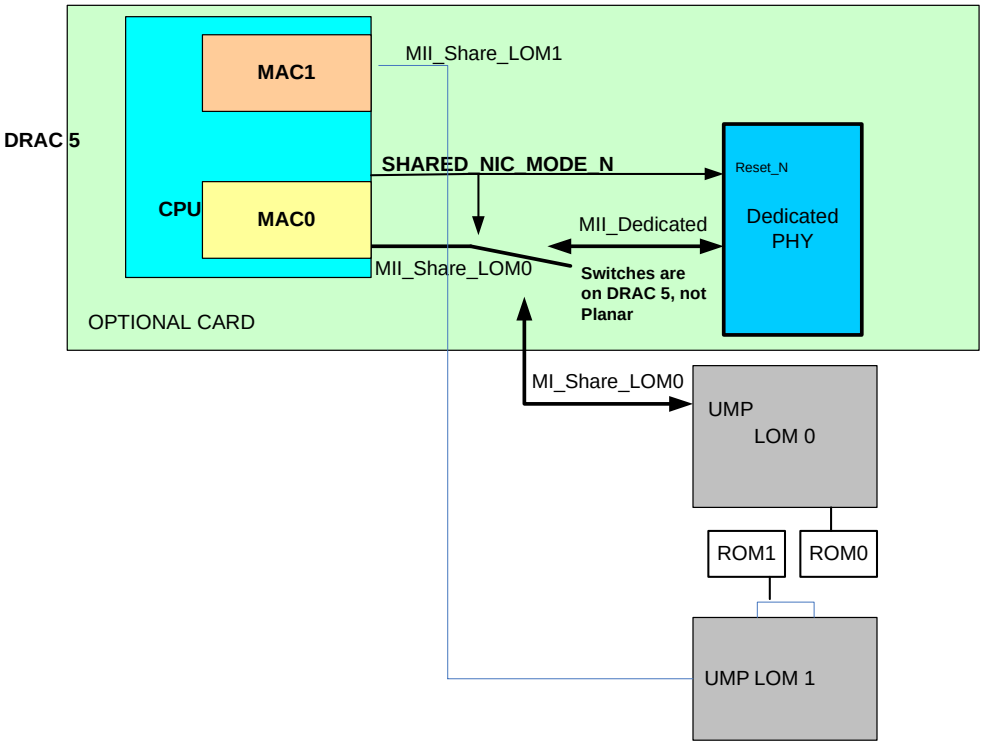

Figure 3: Shared NIC Architecture

DRAC 5 also supports a tagged VLAN. All devices in the VLAN appear to be on the same network segment which allows having DRAC 5 on a separate network segment. Some customers may be

reluctant to use the shared NIC feature because they want to separate regular host traffic from management traffic; if so, they can use VLANs to segment the traffic.

Web Browser Security

The browser connects to our web server via the HTTPS port. All the 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. DRAC 5 ensures 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 5. 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 5 through its network interface, and it uses an HTTPS channel to communicate with DRAC 5. 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 5 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 5 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 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 5 including configuration, power management, firmware update, debug, and so on.

SSH Security

The SSH service is enabled by default on DRAC 5. RACADM CLI can be run in SSH. SSH service can be disabled via DRAC 5 configuration setting. DRAC 5 only supports SSH version 2.

DRAC 5 supports DSA and the RSA host key algorithm. A unique 1024-bit DSA and 1024-bit RSA host key is generated during a DRAC 5 first time power on.

DRAC 5 SSH:

- Supports SHA-1 and MD5 hash algorithms
- Supports the diffie-hellman-group1-sha1 key exchange algorithm
- Supports DSA and RSA public key (asymmetric encryption) algorithms
- Supports 3DES-CBC, blowfish-cbc, cast128-cbc, and rc4-cbc symmetric encryption

- Only supports password user authentication
- Provides a default authentication timeout of 2 minutes
- Provides six authentication attempts as a default

SNMP Security

An SNMP agent runs on a DRAC 5 by default. The DRAC 5 SNMP agent is used by Dell OpenManage™ IT Assistant or other management frameworks to discover the DRAC 5 out-of-band service point, for example, a web GUI URL. DRAC 5 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 5 (for example, service tag of a system or IP address of DRAC 5, and so on).

Dell strongly recommends using one of the following options to secure your DRAC 5 card from these concerns:

- If the DRAC 5 SNMP agent is not being used in your environment, administrators can disable the DRAC 5 SNMP service.
- Change the DRAC 5 SNMP community name to secure their SNMP service. The default DRAC 5 SNMP community name is “public.”
- Limit inbound SNMP access by only accepting specific client traffic by configuring the DRAC 5 allowed client IP address range.

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 5 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 DRAC 5 firmware. The DRAC 5 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 via a 128-bit RC4 key and key exchanges via SSL, if an encrypted connection is selected. To keep virtual media operation going and still have session idle timeout security, DRAC 5 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.

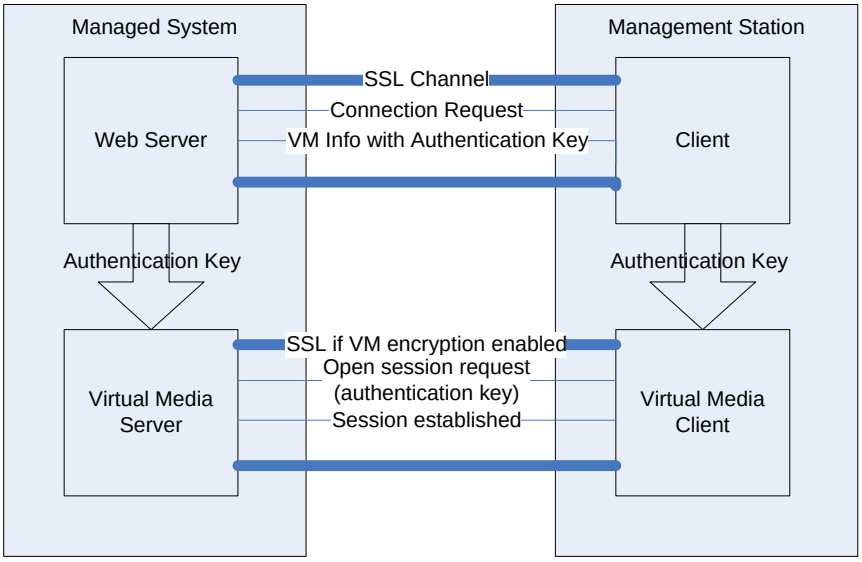

Figure 4: Virtual Media Architecture

Console Redirection Security

Authentication and Encryption

DRAC 5 can continuously redirect the managed system's video, keyboard and mouse (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 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 DRAC 5 web server via the HTTPS channel (SSL encrypted).

3) The DRAC 5 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).

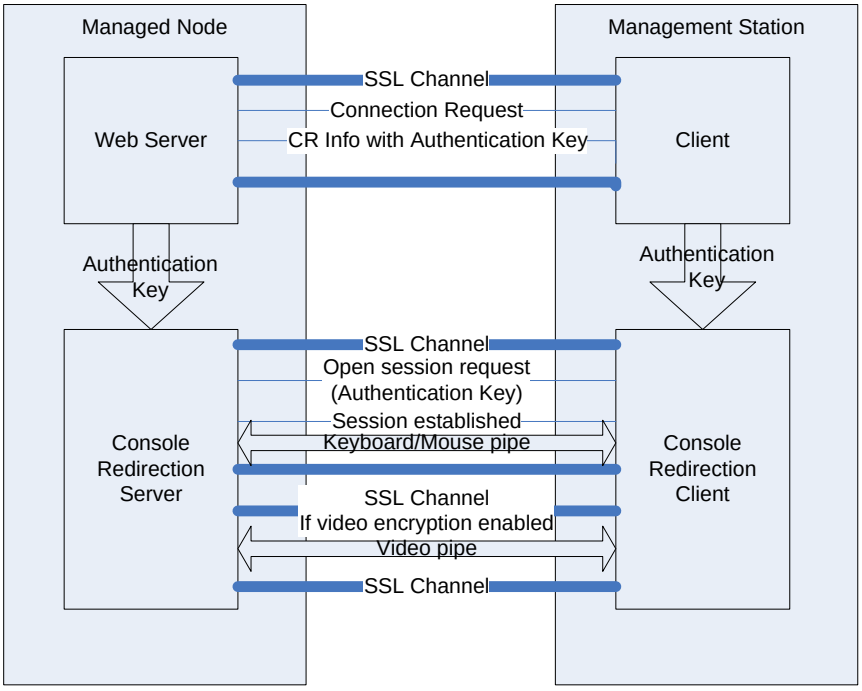

Figure 5: Console Redirection Architecture

User Session Privacy

User session privacy is a security concern in the console redirection feature in DRAC 5.

DRAC 5 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 your console redirection session.

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.

Dell strongly recommends using the Blank Local Video feature if local access is not required during remote console redirection.

NOTE: Requires DRAC 5 version 1.20 firmware or later.

- 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.

Dell strongly recommends disabling console redirection during local RACADM usage if simultaneous remote access is not required.

- In addition to DRAC 5 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 documentation.

IPMI Out-of-Band Access Security

DRAC 5 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 your environment.

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 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.