iDRAC Service Module-iDRAC Access via Host Operating System

This White Paper provides information about the usage and troubleshooting of iDRAC Access via the Host Operating System feature in iDRAC Service Module v2.3 or later.

Dell Engineering
July 2016

Rajib Saha

Bharath Koushik

Sathish Ponnusamy

A Dell Technical White Paper

A Dell Technical White Paper

Revisions (required)

Date	Description
July 2016	Initial release

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Copyright © 2016 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of contents

Executive summary

The Dell Integrated Remote Access Controller (iDRAC) Service Module is a lightweight systems management application installed on a physical Host operating system (OS) of a managed server.

iDRAC Service Module works as a system management application for Dell's Out of Band (OOB) system management processor such as the iDRAC. Installing iDRAC Service Module v2.3 or later allows you to access iDRAC remotely through the host OS without configuring the iDRAC explicitly.

This feature enables you to access iDRAC using the iDRAC supported web interfaces, such as, iDRAC GUI, WSMAN, Redfish and remote racadm. You can continue to use the same iDRAC credentials; if it was configured earlier. If not; you can connect to iDRAC using the default iDRAC credentials.

Warning: Default iDRAC user credentials can be a security threat while using "iDRAC Access via Host OS" feature. It is advisable to change the default iDRAC user credentials before enabling and using this feature.

You can enable the feature during custom installation of iDRAC Service Module through the interfaces supported by iDRAC. By default, the feature is disabled.

Prerequisites for accessing iDRAC via Host OS

- iDRAC Service Module should be installed on the server Operating System.
- The iDRAC Service Module should be running.
- *iDRAC Access via Host OS* feature should be enabled.

Supported Dell Servers or Platforms

- All the Dell 12G PowerEdge servers or later.

Supported Operating Systems

- All Windows and Linux OS variants supported by iDRAC Service Module 2.3.0 version.

Limitations

- When you try to login to the iDRAC console using the 'iDRAC Access via Host OS' feature; audit trails on the LCL does not capture the actual end-user. And there is another log added by iDRAC Service Module to explain the context of iDRAC Access via Host OS with the end-user address.
- Virtual console and Virtual Media are not supported over iDRAC Access via Host OS.
- iDRAC user needs to be configured.
- Asynchronous operations are not supported over iDRAC Access via Host OS only Config. (i.e iDRAC network not configured)

    - SNMP traps (unless iDRAC Service Module is supporting this via "Receive SNMP Trap from OS" feature).
    - Email notifications.
    - WSMAN eventing.
- iDRAC Auto update.
- The iDRAC OS-to-iDRAC Passthru over USBNIC being a 10Mbps channel, iDRAC Access via Host OS may incur delays to operations requiring high bandwidth; such as LC updates.
- Console iDRAC integration (OME/OMPC/Tejas etc..) is not supported over iDRAC Access via Host OS in this release.
- Only IPV4 addresses are supported.

1 Initial Installation

This feature is disabled on a typical or default iDRAC Service Module installation. You can enable the feature during custom installation of iDRAC Service Module through the interfaces supported by iDRAC. The Microsoft IP Helper Service is required for this feature to function.
A port number is required to connect to iDRAC, using which user can connect to iDRAC.This port number is the listening port on the Host OS. In other words, the OS listen for connections on this port which will be redirected to the corresponding iDRAC interface. This configuration of redirecting the connection to iDRAC is done by iDRAC Service Module. Any conflict in the port number should be resolved by the user with administrator privileges.

After providing a valid listen port number; iDRAC Service Module creates a new In-Bound firewall rule (In windows **refered as OS2iDRAC)**. The port number is added to the firewall rule in the Host OS .

This firewall rule is in disabled state by default. You have to to review and enable the rule in the firewall options.

2 iDRAC Access via Microsoft Windows Operating Systems

If the feature is enabled using the custom installation from the .msi file; then an entry into the Network Address Translation rules is created, which can be viewed using the following command:

netsh interface portproxy show all

Listen on ipv4: Connect to ipv4:

Address Port Address Port

--- --- --- ---

* 1234 169.254.0.1 443

Also, an outbound firewall rule by name "OS2iDRAC" is created by iDRAC Service Module. The status of the firewall is disabled by default. You have to to review and enable the rule. The following command shows the status of the firewall rule.

Note: Starting iDRAC Service Module 2.4.0; the firewall rule "OS2iDRAC" is enabled when this feature is enabled. No user action is required in order to access iDRAC via the Host OS.

netsh advfirewall firewall show rule name=OS2iDRAC

Rule Name: OS2iDRAC

Enabled: No

Direction: In

Profiles: Domain,Private,Public

Grouping:

LocalIP: Any

RemoteIP: 10.94.38.1/32

Protocol: TCP

LocalPort: 1234

RemotePort: Any

Edge traversal: No

Action: Allow

Ok.

The firewall rule indicates the port number used during the installation time or user modified port number using the iDRAC Service Module provided interfaces.

To access the iDRAC GUI, use the following format in the browser: *https://<host-name or OS-IP>:9999/login.html*

Where:

Host-name is the complete host-name of the server host OS where iDRAC Service Module is installed and configured for iDRAC access via OS. In the absence of hostname, the OS IP address can be used.

9999 is the host OS port number for accessing the iDRAC through host OS. iDRAC Service Module configures this port, such that all incoming connections is redirected to iDRAC https port (default port is 443). The iDRAC https port number can be modified by the administrator using any of the iDRAC supported interfaces such as racadm, GUI, WSMAN, and so on. iDRAC Service Module is resilient for this change and reconfigures the iDRAC access rules seamlessly without any user intervention.

Remote Wsman: winrm e http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_CPUView -u:<username> -p:<passwd> -r:https://<Host-Name or IP>:<PortNumber>/wsman -a:basic -encoding:utf-8 -skipCACheck –skipCNCheck

Remote racadm: racadm -r <Host Name or IP>:<port#> -u <username> -p <passwd> getsysinfo

iDRAC Service Module provides interfaces to configure this feature runtime.

2.1 *PowerShell configuration*

If this feature is already configured, it can be disabled or modified using the PowerShell cmdlet with the corresponding options.

Pre-requisites for cmdlet

1. Microsoft .NET Framework 64-bit 2.0 or later version.
2. PowerShell 1.0 or later.
3. ExecutionPolicy should be AllSigned or Unrestricted.
    a. Example: To view the current ExecutionPolicy, PS:\> Get-ExecutionPolicy.
    b. To modify: PS:\> Set-ExecutionPolicy AllSigned or Unrestricted.

The cmdlet: **Enable-iDRACAccessHostRoute**

NOTE: In Windows Server 2012 and later; an OS provided help for the cmdlet is available which can be viewed using PS:\> **Get-Help Enable-iDRACAccessHostRoute**

This displays the list of options available and its usage.

The available options are:

1. **Status:** The values are not case sensitive. This parameter is mandatory.
   Values Range {TRUE, FALSE}

2. **Port:** This is the port number and is similar to what user is prompted for during iDRAC Service Module installation. This parameter is mandatory, if the previous parameter "Status" is TRUE. If the Status value is FALSE; then the rest of the parameters can be ignored. If the new port number entered is already configured for this feature; then user is requested to enter a different port number. The existing OS2iDRAC in-bound firewall rule is overwritten with this new port number settings. There-after user have to connect to iDRAC using this new port number.
   Values Range {1024 to 65535}

3. **IPRange:** This parameter is optional irrespective of the other two parameters. This depicts a range of source IP addresses that are permitted to connect to iDRAC via the Host OS. The IP address range format is CIDR format which is a combination of IP Address and Subnet Mask. Any other client outside this specified range is not allowed to connect to iDRAC via Host OS.
   Example: 10.10.10.10/24

This parameter, if specified is added to the Scope variant of the OS2iDRAC firewall rule.

NOTE: Ensure valid and reachable IP Range is specified. Else, iDRAC will not be accessible.

Sl. No.	OS2iDRAC configuration type	Example Command/Syntax
1.	Enable the feature	Enable-iDRACAccessHostRoute –status true –port 1234
2.	Listen Port Modification	Enable-iDRACAccessHostRoute –status true –port 2345
3.	Adding IP Range or Whitelist IPs	Enable-iDRACAccessHostRoute –status true –port 2345 –iprange <10.10.10.3/24>
4.	Disabling the feature	Enable-iDRACAccessHostRoute –status false

Any modification to the listen port number can modify the firewall rule "OS2iDRAC" and it can be disabled. This must again be reviewed by the administrator and enabled as necessary.

NOTE: Disabling this feature removes the OS2iDRAC firewall rule from the list.

NOTE: Enabling or disabling this feature can create an audit log entry in the OS logs (Event Viewer.)

Like the PowerShell way of specifying IPRange values, iDRAC also supports Network Security to allow restricted clients to connect to iDRAC. If the allowed IP Range is already configured in iDRAC before iSM installation; then iSM shall configure the same on the Host OS as well for iDRAC Access via Host OS feature. Any subsequent modification of IP Range in iDRAC shall not take effect. In other words, the IP range specified using the iDRAC Service Module provided command line interfaces take precedences over the iDRAC IP Range Setting.

3 iDRAC Access via Linux Operating Systems

After adding a valid listen port number; iDRAC Service Module adds Destination Network Address Translation (DNAT) and Source Network Address Translation (SNAT) rules which redirects the connections on the user configured listening port to iDRAC. There is an additional NAT rule added in the PREROUTING Chain to block the incoming connections on the listening port. The administrator is expected to validate the newly added NAT rules and delete the blocking rule in order to activate iDRAC access feature through host OS IP. The blocking NAT rule is configured as shown here.

iptables -t nat –L

target prot opt source destination

RETURN tcp -- anywhere anywhere tcp dpt:<listen-port>

The rule can be removed with the following command:

iptables -t nat -D PREROUTING -p tcp --dport <listen-port> -j RETURN

These are the basic configurations required to access iDRAC interfaces through the OS. To access the iDRAC GUI, use the following format in the browser: **https://<host-name or OS-IP>:<listen-port>/login.html**

NOTE: For details on how to configure SNAT and DNAT rules, refer: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Security_Guide/s1-firewall-ipt-fwd.html. The configuration may vary based on the Linux distribution used.

3.1 Configuration using Linux Command line

The administrator has the option of enabling or disabling this feature using the iDRAC Service Module provided Linux Command Line Executable file . Also if this feature is already configured, it can be disabled or modified using the Command Line.

The Command Line Executable Name: **Enable-iDRACAccessHostRoute.**

The command

 # /opt/dell/srvadmin/iSM/bin/Enable-iDRACAccessHostRoute

Usage

./Enable-iDRACAccessHostRoute <Enable-Flag> [<source-port> <source-IP-range/source-ip-range-mask>]

Where:
<Enable-Flag>: Possible values are 0 for Disable and 1 for Enable
<source-IP-range>: should be in the format of <IP-Address/subnet-mask>. For Example, 10.95.146.98/24

NOTE1: If <Enable-Flag> value is 0, the parameters <source-port>, <source-IP-range/source-ip-range-mask> is not required.

NOTE2: If <Enable-Flag> value is 1, then the <source-port> is Mandatory. <source-IP-range> <source-ip-range-mask> parameters are optional.

NOTE3: Currently, only IPV4 addresses are supported for this feature.

Examples

1. To disable the feature:
   [root@MyDevBox bin]# **/opt/dell/srvadmin/iSM/bin/Enable-iDRACAccessHostRoute 0**
   iDRAC access via Host OS feature configuration has been disabled.
   After the feature is disabled, iDRAC Service Module deletes all the newly added DNAT and SNAT rules.

2. To Enable the feature or to change the listening port number:

   [root@MyDevBox bin]# **/opt/dell/srvadmin/iSM/bin/Enable-iDRACAccessHostRoute 1 9999**

   iDRAC access via Host OS feature configuration has been updated successfully. Please verify and enable the Firewall rule for OS2iDRAC feature to work. You can access iDRAC using the port number specified. For example, use https://<hostname>:5678/login.html to access the iDRAC web interface.

   The feature is enabled and the new port number **9999** is configured as the listen-port number.

   The newly added NAT rules are:

   [root@MyDevBox bin]# **iptables -t nat -L**
   Chain PREROUTING (policy ACCEPT)
   target prot opt source destination
   RETURN tcp -- anywhere anywhere tcp dpt:**9999**
   DNAT tcp -- anywhere anywhere tcp dpt:**9999** to:169.254.0.1:443

   Chain POSTROUTING (policy ACCEPT)
   target prot opt source destination
   SNAT tcp -- anywhere 169.254.0.1 tcp dpt:https to:169.254.0.2

3. To Enable the feature with IPRange setting:

   [root@MyDevBox bin]# **/opt/dell/srvadmin/iSM/bin/Enable-iDRACAccessHostRoute 1 9999 <10.10.10.10>/16**

   iDRAC access via Host OS feature configuration has been updated successfully. Please verify and enable the Firewall rule for OS2iDRAC feature to work.
   You can access iDRAC using the port number specified. For example, use https://<hostname>:9999/login.html to access the iDRAC web interface. Now the feature is enabled with listen port number 9999 and only for the Source IP addresses in the range 10.10.10.10/16.

   The newly added NAT rules are:
   [root@MyDevBox bin]# iptables -t nat -L
   Chain PREROUTING (policy ACCEPT)
   target prot opt source destination
   RETURN tcp -- anywhere anywhere tcp dpt:**5678**

```
DNAT       tcp  --  10.11.0.0/16        anywhere             tcp dpt:5678 to:169.254.0.1:443

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
SNAT       tcp  --  anywhere            169.254.0.1          tcp dpt:https to:169.254.0.2
```

4 Troubleshooting and Recovery

4.1 Failure to access iDRAC via Host OS due to Iptables holding the lock in Linux OS

Symptoms

While trying to access iDRAC page via Host OS, it fails to connect to iDRAC page and throws the error "The site can't be reached."

Reason

When executing, Iptables acquires an internal lock and if multiple iptables commands are run simultaneously, one of the commands might fail as the other command had acquired the lock already. The iDRAC Access via Host OS feature fails to configure when there is an iptables command running which already have acquired the lock.

Recovery Action

By verifying if the SNAT and DNAT rules are configured with the given port, it can be confirmed if the iDRAC Access via Host OS feature is configured properly or not.

```
[root@MyDevBox bin]# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  10.10.0.0/16        anywhere            tcp dpt:9999 to:169.254.0.1:443

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
SNAT       tcp  --  anywhere            169.254.0.1         tcp dpt:https to:169.254.0.2
```

If the DNAT and SNAT rules were not added, the other instances of iptables command needs to be stopped and using CLI the feature needs to be reconfigured again.

4.2 Failure to access iDRAC via Host OS due to disabling of IP Forwarding in Linux kernel

Symptoms

While trying to access iDRAC page via Host OS, it fails to connect to iDRAC page and displays the error "The site can't be reached."

Reason

IP Forwarding is a concept to make Linux based machines to send data from one network to other. In order to forward the connection request to iDRAC, the host OS should enable IP Forwarding in the kernel.

If it is disabled iDRAC Access via Host OS feature fails.

Recovery Action

It can be enabled using the command

"echo 1 > /proc/sys/net/ipv4/ip_forward"

4.3 Failure to access iDRAC via Host OS due to a Firewall rule that is configured by some other application to block the listen port

Symptoms

While trying to access iDRAC page through Host OS, it fails to connect to iDRAC page and throws the error "The site can't be reached."

Reason

There are scenarios where there is other firewall rules from other applications that has blocked the listen port that is configured for iDRAC Access via Host OS.

Recovery Action

The port has to be unblocked or a new port has to be configured for this feature to work. If firewall is enabled after iDRAC Access via host OS configuration then re-configure the iDRAC Access via Host OS with valid port. For more information on enabling iDRAC via Host OS, refer the **Configuration using Linux Command line** section.

4.4 Failure to access iDRAC via Host OS due to a Firewall rule is configured to block the IP

Symptoms

While trying to access iDRAC page through Host OS, it fails to connect to iDRAC page and displays the error "The site can't be reached."

Reason

There are scenarios where there is other firewall rules from other applications or administrator that has blocked the Source IP that is configured for accessing iDRAC via Host OS.

Recovery Action

The IP Address has to be unblocked for accessing the iDRAC from that Source IP.

4.5 Failure to access iDRAC via Host OS during iDRAC reset

Symptoms

While trying to access iDRAC page via Host OS, it fails to connect to iDRAC page and displays the error "The site can't be reached."

Reason

When iDRAC reset is in progress, it fails to access the iDRAC via Host OS until it comes up.

4.6 Failure to access iDRAC via Host OS while iDRAC is unavailable

Symptoms

While trying to access iDRAC page via Host OS, it fails to connect to iDRAC page and displays the error "The site can't be reached."

Reason

When the iDRAC Firmware update is in progress, accessing iDRAC via Host OS fails. Only after the iDRAC comes up, the user is able to access the iDRAC.

4.7 Failure to access iDRAC via Host OS due to iDRAC Network Security Settings

Symptoms

While trying to access iDRAC page via Host OS, it fails to connect to iDRAC page and displays the error "The site can't be reached."

Reason

After a successful first time configuration of "iDRAC Access via Host OS" using the iDRAC Service Module webpack; the iDRAC interfaces may not be reachable due to default NetworkSecurity settings in iDRAC irrespective of whether default NetworkSecurity settings is enabled or not.

Recovery Action

This can be overcome by reconfiguring "iDRAC Access via Host OS" using the PowerShell cmdlet or Linux CLI. The IPRange can be set using the cmdlet as shown in the example command below:

On Microsoft Windows:
Enable-iDRACAccessHostRoute -status true -port 12345 -IPRange 10.94.146.5/24

On Linux OS es:
./Enable-iDRACAccessHostRoute 1 12345 10.94.146.5/24

The IP Range value must follow the CIDR format.

4.8 Failure to access iDRAC via Host OS due to iptables filter FORWARD rule on RHEL 7.2 and SLES12 SP1 OS es

Symptoms

While trying to access iDRAC page through Host OS, it fails to connect to iDRAC page and throws the error "The site can't be reached."

Reason

After a successful first time configuration of "iDRAC Access via Host OS"; the iDRAC interfaces may not be reachable due to the iptables filter FORWARD rule created by the FIREWALLD.SERVICE in the Host OS to reject all packets by default. The issue is only observed in RHEL 7.2 and SLES12 SP1 OSes.

Recovery Action

If the FORWARD chain is configured to DROP/REJECT packets for all or the iDRAC USBNIC IP/iDRAC Secure port (e.g.169.254.0.1/ 443), the administrator have to create a new FORWARD chain to allow packets destined for iDRAC IP and port. You can create the new FORWARD chain by using the following command:

iptables -N OS2iDRAC
iptables -I FORWARD -j OS2iDRAC
iptables -A OS2iDRAC -p tcp -d 169.254.0.1 --dport 443 -j ACCEPT

iptables -A OS2iDRAC -p tcp -i idrac -s 169.254.0.1 -j ACCEPT

(By Default, the iDRAC USBNIC IP is 169.254.0.1, iDRAC Secure Port is 443). The iDRAC USBNIC IP and iDRAC Secure Port details can be obtained from the file /opt/dell/srvadmin/iSM/etc/ini/dcos2idrac.ini as mentioned below.

```
connect_address=169.254.0.1
connect_port=443
```

4.9 iDRAC Access via Host OS feature can't be enabled post installation if it is not included manually during installation using webpack

Symptoms

While trying to access iDRAC page via Host OS, it fails to connect to iDRAC page and displays the error "The site can't be reached."

Reason

While installing iDRAC Service module using the *setup.sh* provided as part of the Linux webpack and if the user does not select the "iDRAC Access Via Host OS" feature to install, it is observed that you cannot enable the feature post installation.

Recovery Action

Modify the iDRAC Service Module by running *setup.sh* installer script, with the option to enable "iDRAC Access via Host OS" feature as mentioned below.

./setup.sh -i -O --port=<listen-port-no>

Where:

––port is a mandatory parameter. This port number is used to listen for connections/requests to iDRAC on the Host OS, in order to forward all connections or requests to iDRAC.

Accepted port number range is 1024 to 65535. You must ensure that a unique port number is assigned. This issue is not observed when the iDRAC Service Module is installed using the other alternative methods such as iDRAC Service Module DUP, yum, and rpm packages. The feature can be configured using the "Enable-iDRACAccessHostRoute" CLI.

4.10 Failure to access iDRAC via Host OS on Microsoft Windows although the listen port and firewall are configured

Symptoms

While trying to access iDRAC page via Host OS, it fails to connect to iDRAC page and displays the error "The site can't be reached."

Reason

The Microsoft Windows service “IP Helper” is required for this feature to function. Ensure this service is running on your Managed Node, where iDRAC Service Module is installed.

Recovery Action

If the “IP Helper” service is stopped, start the “IP Helper” service on the Managed Node where iDRAC Service Module is installed.