Dell™ iDRAC Quick Sync

Overview

Sajjad Ahmed
Dell | Quick Sync HW Architect
Portfolio Design Group
November 2014

A Dell Technical White Paper

Revisions

Date	Description
November 2014	Initial release

Table of Contents

1.   Introduction

This document serves as a hardware technical guide for the optional integration of the Near Field Communication (NFC) technology into Dell's 13th generation PowerEdge servers – specifically the R730, R730xd, R630, and R7910 models.

2.   What is the iDRAC Quick Sync feature?

Dell has introduced an iDRAC Quick Sync optional feature with certain 13th generation PowerEdge servers. This innovative solution utilizes the Near Field Communication (NFC) technology to enable customers' mobile workforce to bridge the gap between mobility and server management.

For customers managing servers directly in the data center, this new capability transmits server health information and basic server setup by using a hand-held smart device running the OpenManage Mobile (OMM) application, simply by tapping it at the server. OMM also enables administrators to monitor and manage their environments anytime, anywhere using their mobile device.

3.   What is NFC?

3.1   Overview

NFC is a set of standards for smartphones and similar devices to establish two-way communications with each other by touching or bringing them in close proximity to each other, usually not more than a few centimeters. NFC complements several popular wireless technologies, by utilizing the key elements in existing standards for contactless card technology (ISO/IEC 14443 A&B and JIS-X 6319-4). NFC operates at 13.56 MHz and can support data transfer rates of up to 848 kbps. NFC's bidirectional communication ability is ideal for authentication and for establishing connections with other technologies with a simple tap.

3.2   How NFC works

NFC uses the basic principle of magnetic field induction and relies on the mutual coupling between the devices. An NFC device either creates its own magnetic field or uses the fields generated by another NFC device to power itself. A device that generates its own field is called an active device and is said to be in the active mode. If a device uses the field of another NFC device to generate its power, it is usually called a passive device and is set to be in the passive mode. Besides active and passive modes, there are two different roles NFC devices can play in an NFC communication, the first being Initiator and the second being Target. Since NFC is based on a query and respond concept, it is not possible for two devices to send data at the same time. In other words, the first device must receive a request for data from the second device and only then will the first device send data to the second device. Because of this communication method, a passive device cannot initiate communications.

Table 1. NFC Operation Modes

Mode Type	Device Type	
	Active	Passive
Initiator	Supported	Not Supported
Target	Supported	Supported

In order to function, the initiator device sends out a signal to the target. If both the devices are in close proximity, they will create a high-frequency magnetic field between the loosely coupled coils in both the initiator device and the target. Once this field is established, a connection is formed and information can be passed between the initiator and target by fluctuating the magnetic fields. Target receives the instruction and checks if it is valid. If not, nothing occurs. If it is a valid request, then the target responds with the requested information.

3.3 Applications of NFC

NFC can be used in many different ways. In the Finance sector, NFC is being used in point-of-sale (PoS) applications. Content access, access control, authentication applications, medical applications, advertising, consumer electronics, and transportation are other areas where NFC is being utilized.

3.4 The rationale for using NFC in iDRAC Quick Sync

Adoption of NFC technology is on the rise and it is expected to be available on ~575 million smart phones by 2015 according to IDATE (http://www.nfcworld.com/2014/07/15/330373/idate-forecasts-nfc-phones-payments-volumes/). NFC technology was mainly targeted at mobile payment transactions and hence is built from the ground up to be the most secure technology. Dell internal market research shows that more than 60% of customers perform various management activities at the datacenter in front of the server. Using the iDRAC Quick Sync mobile interface to manage servers at the data center improves business productivity by enabling 55% faster iDRAC configuration and 84% faster server information retrieval.

4. Security with NFC

NFC is one of the most secure wireless technologies in the industry. As a consumer, it is imperative to understand the limitation of NFC as well as the benefits of NFC over the high bandwidth wireless, such as WiFi and Bluetooth. Following are some of the ways data can be compromised, and rationale behind using NFC in Quick Sync feature.

4.1 Data Modification

In this type of threat, the receiver of data receives the valid but modified data. This type of attack is contingent on the amplitude modification of the signal.

NFC can inherently detect the increase in power from what is required for normal communication and stop the transmission automatically.

4.2 Data corruption

In this type of threat, instead of just listening the attacker modifies the transmission in order to disrupt the communication. It is a form of Denial of Service (DOS) and the attacker might need to be aware of the technology in order to transmit at valid spectrum of frequencies and at the right time.

NFC devices are capable of checking the magnetic field while transmitting the data. Attach can be detected since the power required to corrupt the data is significantly larger than normal communication and NFC devices can stop transmission.

4.3 Man-in-the-middle

This is a classic type of intrusion and requires the attacker to act like a middle man while two NFC devices are communicating with each other. The attacker can then read and manipulate the data before relaying it to the intended device.

Due to the requirement of the proximity of NFC it is almost impossible to do a man-in-the-middle type of attack. NFC is also capable to detecting disturbance in its magnetic field and can turn off its transmission.

4.4 Eavesdropping

Since NFC is a form of wireless communication, eavesdropping is a major concern. It is imperative for customers to understand the limitations and advantages of the NFC technology from the prospective to eavesdropping. NFC communication is done between two devices that are in close proximity with a typical distance of 10 cm or less between the two devices. Because of this proximity, it becomes challenging to gauge the distance required for the attacked to be able to retrieve a usable data from NFC transmission. There are large numbers of parameters that need to be taken into account, for this type of attack to succeed. Characteristics of the victim device (like antenna strength, magnetic shielding, and other environmental variables), characteristics of aggressor's device (like antenna strength, magnetic shielding, and other environmental variables), quality of victim's and aggressor's antenna and NFC power setting in both the devices are the examples of such parameters. Since NFC uses magnetic field induction, presence of metallic components in the surroundings will also hinder the attack.

Data in Quick Sync is intelligently encrypted using Diffie-Hellman and symmetric cryptography providing security even in the event of a complete compromise of the iDRAC Quick Sync bezel. iDRAC Quick Sync is designed to operate at 3 cm (nominally) and employs an inactivity based timeout feature that completely turns off the iDRAC Quick Sync feature when there is no activity detected. iDRAC Quick Sync is further made secure by requiring activation button to be pressed in order to turn on and get the bezel ready for interaction with mobile device before it times out again and turns off the NFC transmitter.

5.   Quick Sync enablement

5.1 Server Hardware

For now, Quick Sync feature is supported in 13th generation PowerEdge R630, R730 and R730xd servers. The supported server must have the Quick Sync enabled rack ears as shown in Figure 1.

Figure 1: Quick Sync enabled rack server's "ear"

A Quick Sync enabled bezel is also required for this feature to be functional.

Figure 2: Quick Sync-enabled bezel

Figure 3: Close up of iDRAC Quick Sync-enabled bezel

5.2   Mobile Device

The mobile device must be running an Android Operating System 4.0.3 or higher; must be equipped with NFC technology and must have Dell OpenManage Mobile app installed. The app can be downloaded for free from the Google play store. (https://play.google.com/store/apps/details?id=com.dell.omm&hl=en).

6.   Hardware features of iDRAC Quick Sync

The iDRAC Quick Sync-enabled bezel contains an antenna, notification LEDs, an Activation Button and interconnects to the server. Figure 4 below shows all of these features.

6.1   Activation Button

The button labeled "Activation Button" in Figure4must be pressed to activate the iDRAC Quick Sync feature. This has been designed to provide additional security by requiring physical presence of a user at the box. This button also allows a user to distinguish between an activated and non-activated bezel so that a user can interact with the appropriate server. Once activated, the Quick Sync feature will time-out after 30 sec. The time-out is configurable via the server's iDRAC. Pressing this button while Quick Sync is activated will deactivate the Quick Sync bezel.

6.2   Antenna

Since NFC requires an antenna to function, it is embedded in the perimeter of the window. Besides serving as a guide for NFC antenna, this open window also helps with the server's airflow. Status bar

The Activation Button and Status Bar share the same LED. The Status Bar will light up the LED to let a user know which system is active and that its Quick Sync feature is ready for use. The Status Bar can also be used to troubleshoot the Quick Sync feature as explained in the Troubleshooting section.

6.3   Bezel interconnect

The Quick Sync bezel interfaces with a server using a group of six pogo pins that connect to the rack server's "ears" – the left and right edges of the front panel of the rack-mounted server. The bezel has been designed to be handled, but care must be taken while handling the bezel.

7.   Interaction with a server using iDRAC Quick Sync

With an iDRAC Quick Sync bezel inserted in an iDRAC Quick Sync enabled system, launch the OMM app and then press the activation button on the bezel. The activation button and status bar will illuminate with a solid white color. At this point you can interact with the server. Simply tap and hold to transfer information. It will take less than 2 s to transfer the information.

Step 1: Press the Activation button.

Figure 4. Activation button

Step 2: Make sure that status LED is solid, indicating that system is ready

Figure 5. Activated Quick Sync

Step 3: Launch the OMM app on your mobile device.

Step 4: Tap and hold the mobile device for 2 seconds

Figure 6. Tap and hold mobile device

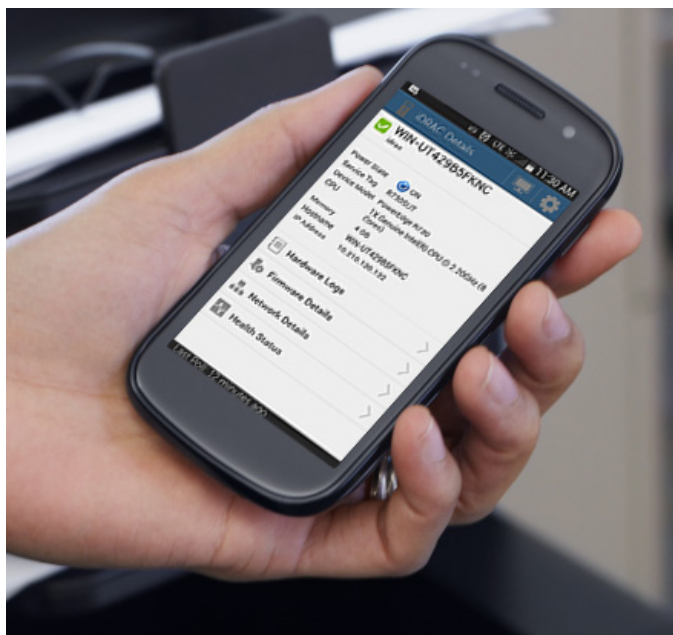Step 5: View/edit the information. Details on how to use OMM are explained here: http://dell.to/1yIcVtc.

Figure 7. Interact with OMM

8.   Data supported via iDRAC Quick Sync

The primary reason to use IDRAC Quick Sync feature is to replace or enhance the user experience over a traditional server LCD panel as a management tool. Traditionally, the LCD panel has proven useful, but the amount of display space is limited and is not optimal for richly-equipped systems. With iDRAC Quick Sync and OpenManage Mobile, you will now have quick access to the following information:

- **Asset Information**

    - Service tag

    - Asset tag

    - System model

- **Host Information**

    - Host CPUs (numbers, model, speed)

    - Host Memory (in GBs)

    - Host name

    - OS name

    - OS version

- **Sensors Information**

    - Power (current consumption)

    - Global Health

- Sub system health
- Inlet temperature
- Exhaust temperature

- **iDRAC Networking Information**
    - IPV4 enable/disable
    - IPV4 DHCP enable/disable
    - IPV4 IP address
    - IPV4 subnet
    - IPV4 Gateway
    - IPV4 DNS settings
    - IPV4 Primary/Secondary DNS
    - IPV6 enable/disable
    - IPV6 Configurations
    - IPV6 DHCPv6 or Static for DNS
    - IPV6 Gateway
    - IPV6 Primary/Secondary DNS
    - iDRAC MAC addresses
    - iDRAC DNS name

- **Host Networking Information**
    - Permanent Ethernet MAC
    - Virtual Ethernet MAC
    - Permanent iSCSI MAC
    - Virtual iSCSI MAC

- **Host Networking Information**
    - Name and version of all the Firmware on the server (ex; iDRAC, BIOS, LC, NIC, PERC)

- **Log access**
    - Last 20 critical and/or all SEL log
    - Last 20 critical and/or all LC log

- **Other data**
    - Boot order list
    - First boot device
    - Boot once flag
    - Reset Root password
    - NFC access configuration

9. iDRAC settings for Quick Sync

9.1 Quick Sync inventory information

Quick Sync will appear as "integrated Quick Sync" under hardware inventory.

9.2 Quick Sync configuration

iDRAC Quick Sync settings are located under Hardware\Front Pane.

9.3 Presence

Presence field lets the user know that a Quick Sync capable bezel is attached to the system.

9.4 Access

1. "Disable" – This mode will disable any communication with iDRAC Quick Sync regardless of input to the activation button or a change in the physical iDRAC Quick Sync hardware.

2. "Read only" – this mode will disable any communication back to the server.

3. "Read-Write" – this configuration allows the flow of communication to and from the server. Any communication to the server will be authenticated first before being accepted by iDRAC.

9.5 Timeout

This is the enable/disable option for time out. When enabled and no activity is detected until the time out limit expires, Quick Sync will timeout and turn off all the hardware for Quick Sync. This provides additional security over NFC and Dell base encryption. The user can choose to disable the time out mechanism. In that case, NFC and the Quick Sync bezel will become active when the Activation Button is pressed and will remain active unless the Activation Button is pressed again.

9.6 Timeout Limit

Indicates the time of inactivity after which the Quick Sync mode is disabled. From the drop-down menu, select seconds or minutes, and then enter the value in the text box. By default, seconds is selected. The default value is 30 s. Range is from 15 s to 3600 s or from 1 minute to 60 minutes.

10. Troubleshooting

The Status Bar on the Quick Sync bezel is also used to notify user with any possible issues with the bezel or server hardware. Following is the LED pattern decoder:

Power indicator pattern	Condition
Slow blink – breathing	Quick Sync is waiting to be configured from iDRAC.
Solid	Quick Sync is ready to transfer.
Blinks three times rapidly and then turns off	Quick Sync feature is disabled from iDRAC.
Blinks continuously when the mobile device touches the antenna	Indicates data transfer activity.
Blinks rapidly five times and turns off for one second when the activation button is pressed. This pattern is repeated until the activation button is pressed again.	Quick Sync hardware is not responding properly. Reseat the bezel. If the problem persists, contact Dell technical support.
Off	Indicates that the Quick Sync feature is turned off. Use the activation button to activate it. If pressing the activation button does not turn on the LEDs, it indicates that power is not being delivered to the Quick Sync bezel.