DELL Technologies

White Paper

Improved security with iDRAC9 using Root of Trust and BIOS Live Scanning

Maintaining best in class security on Dell EMC PowerEdge servers running iDRAC9 4.10.10.10 and 4.40.20.00

Abstract

iDRAC9 4.10.10.10 (AMD platforms) and 4.40.20.00 (Intel platforms) provides an improved Root of Trust mechanism that helps reduce the risk of malware infiltration into sensitive server areas. For newer Intel and AMD platforms, additional BIOS live scanning checks to ensure that no unauthorized changes occur.

June 2021

Revisions

Date	Description
April 2020	Initial release
August 2021	Updated with Intel platforms

Acknowledgments

Authors:

- Aniruddha Herekar
- Arun Muthaiyan
- Doug Iler
- Murali Somarouthu
- Prashanth Giri

Table of contents

Executive summary

Security is critical to the operational success of any data center. Dell EMC is committed to continually improve the code to provide the most secure solution to its customers. The iDRAC9 4.10.10.10 (AMD platforms) and 4.40.20.00 (Intel platforms) firmware release leverages the role of hardware-based security technologies and checks the BIOS for integrity.

Also, BIOS image scanning can be initiated using both schedule and on-demand features. The BIOS live scan feature is only available on 15th generation PowerEdge servers with AMD “Rome” based processors or Intel “Ice Lake” processors.

This document discusses how the iDRAC Root of Trust (RoT) and BIOS live scanning enhances server security.

1 Introduction

Today, even a flashed firmware a Read Only Memory is susceptible for exploitation by hackers. Hackers try to find a way to modify, tamper, or expose a system to malicious activities. While UEFI Secure Boot Mechanism is effective in providing host security, it is not effective avoiding an attack if flashed firmware is compromised. A malicious hacker who has physical access to a system can tamper with the BIOS image. The security threat that a tampered BIOS code poses is high and leaves the system open to further attacks.

To counter the boot integrity threat problem, Intel introduced Boot Guard technology a few years ago with its Fourth-generation cores. This Root-of-Trust is based on one-time programmable, read-only public keys that provide protection against malware tampering. When a system with Boot Guard starts, the cryptographic hash of the BIOS image is verified against the stored key. If the verification succeeds, the BIOS boots as expected. If the verification fails, the BIOS image is compromised, and the system fails to boot.

In addition to Boot Guard's verification mechanism, iDRAC9 provides a Root of Trust mechanism to verify the BIOS image at the host boot time. The host can boot only after the BIOS image is successfully validated. iDRAC9 also provides a mechanism to validate the BIOS image at run time on demand or at user-scheduled intervals.

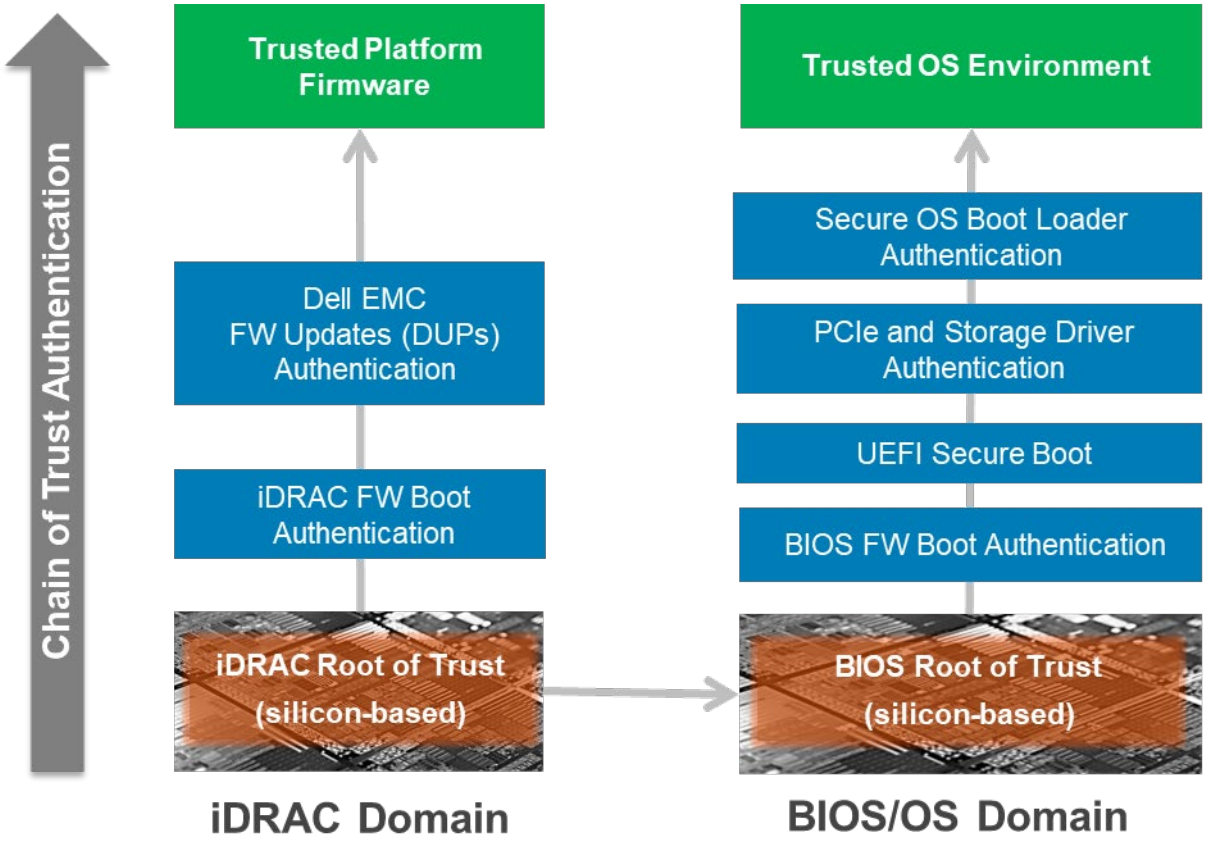


Figure 1 Silicon-based Root of Trust Domains in PowerEdge Servers with iDRAC9.

2 Dell EMC Root of Trust and BIOS live scanning

2.1 Root of Trust

Dell EMC takes security seriously and has adopted Boot Guard technology on its new generation of PowerEdge servers to counter BIOS tampering issues. On the latest Dell EMC PowerEdge servers with iDRAC9, iDRAC first boots with chain of trust authentication, and then verifies BIOS integrity. iDRAC takes on the role of hardware-based security technologies as well. For AMD, the iDRAC9 accesses the primary BIOS ROM through SPI in addition to AMD fusion controller hub (FCH) and performs the RoT process. For Intel, the iDRAC9 accesses the primary BIOS ROM through SPI and Intel Platform Controller Hub (PCH) and performs the RoT process.

iDRAC9 directly accesses the BIOS primary ROM to perform a RoT operation on the processor, on both the security block and the host initial BootBlock.

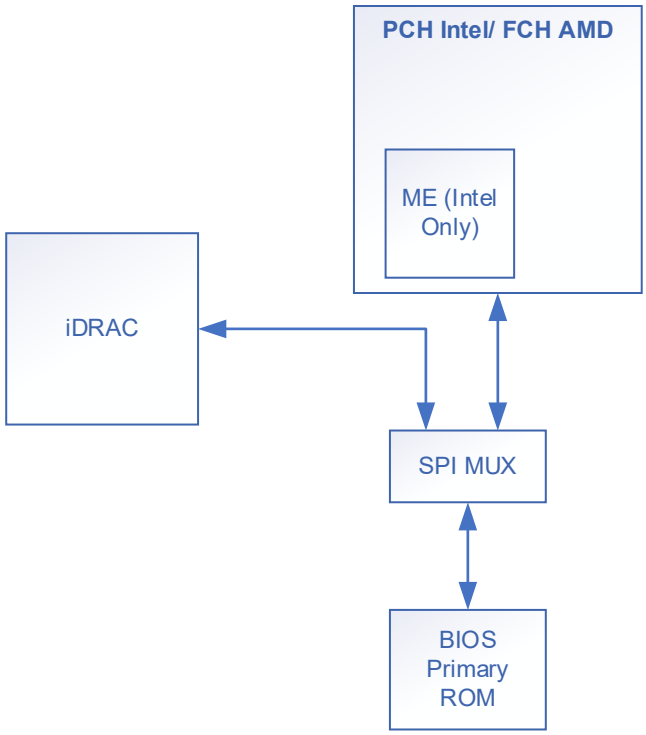


Figure 2 iDRAC accessing BIOS image ROM.

Under the following conditions, iDRAC9 recovers the BIOS.

1. BIOS integrity check failed.
2. BIOS self-check failed.

3. Using RACADM command.
    a. RACADM command:
    racadm recover BIOS.Setup.1-1

2.1.1 Platforms and iDRAC version support

Table 1 Platforms, iDRAC versions, and Features support

Platforms	iDRAC9 versions supported	Features
R6525, C6525	3.42.42.42 and above	BIOS Integrity check at host boot
R6525, C6525, and R7525	4.10.10.10 and above	BIOS Integrity check at host boot and live scanning of BIOS image
Dell's 15th Generation Intel XCC platforms, such as R650, R750, MX750c, and others	4.40.20.00 and above	BIOS Integrity check at host boot and live scanning of BIOS image

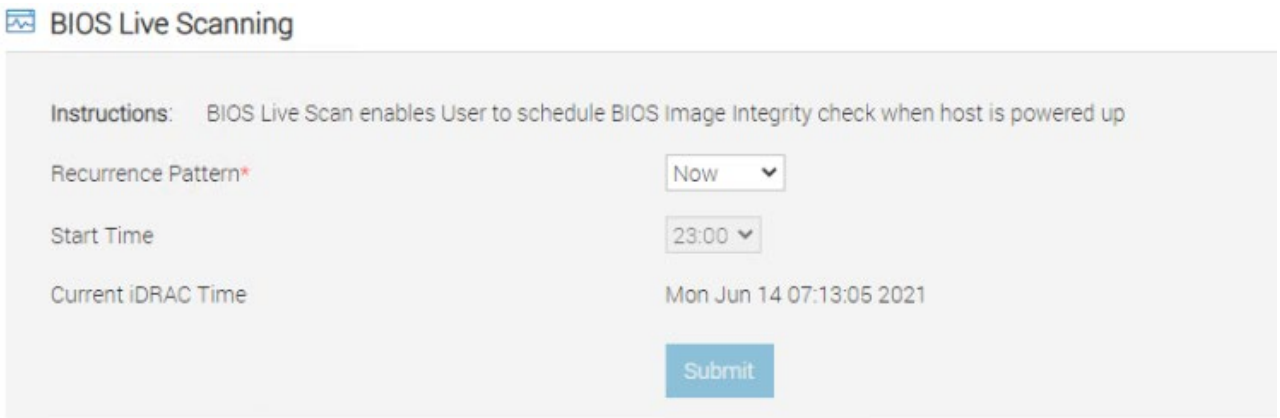
Note: iDRAC9 hardware RoT and BIOS live scanning feature support is available only with Dell's 15th Generation Intel and AMD platforms. See iDRAC9 release notes for supported new generation of platforms.

2.2 BIOS live scanning

BIOS live scanning verifies the integrity and authenticity of the BIOS image in the primary ROM when the host is powered on. BIOS live scanning is not in the POST process. This feature is available only with iDRAC9 4.10.10.10 (supported AMD platforms) and 4.40.20.00 (supported Intel platforms) Datacenter license. You must have administrator privileges, or operator privileges with "Execute Debug Commands" debug privilege to perform this operation. You can schedule the scan through the iDRAC UI, racadm, and Redfish interfaces.

2.2.1 Scheduling a scan using the iDRAC UI interface

The following image shows the various options available to run a BIOS live scan.



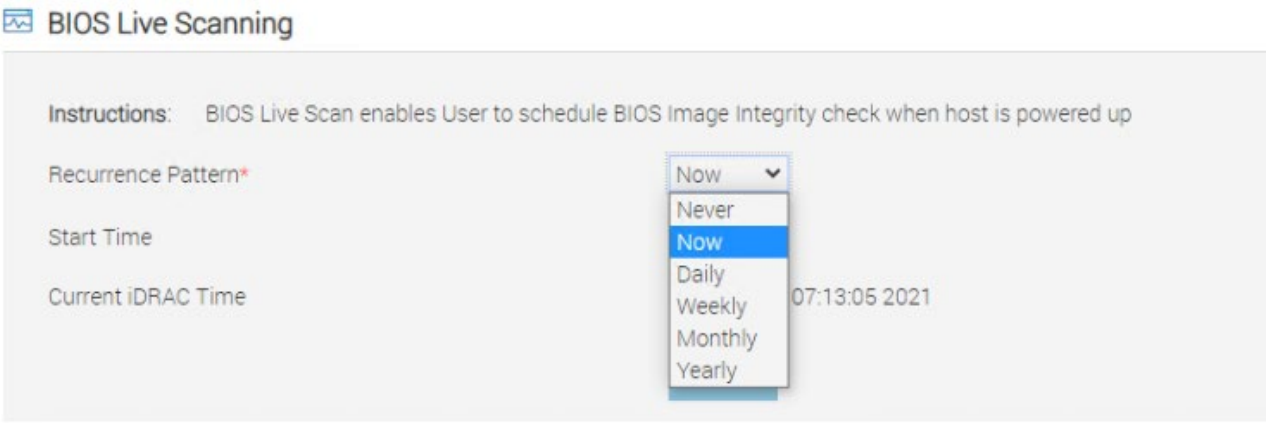


Figure 3 BIOS live scanning options in iDRAC UI.

2.2.2 Scheduling a scan using the RACADM interface

Usage: racadm biosscan -s <start-time>

#racadm help biosscan

Racadm biosscan -- Performs BIOS Live Scanning

Usage:
racadm biosscan -s <start-time>
-s <start-time>
0 - Never schedule. Deletes existing jobs
1 - Schedule Now
2 - Schedule Daily
3 - Schedule Monthly
4 - Schedule Yearly

Usage Examples:
- To perform BIOS scan now:
racadm biosscan -s 1

2.2.3 Scheduling a scan using the Redfish interface

1. First run the **"Get"** command and enter the username and password when prompted.

   https://<IP address>/redfish/v1/Systems/System.Embedded.1/Bios

2. There are two options to run the Post operation to initiate the BIOS live scanning.
   - Post operation with empty payload to **schedule immediate scanning** job.

https://<IP address>/redfish/v1/Systems/System.Embedded.1/Bios/Actions/Oem/DellBios.RunBIOSLiveScanning

- Post operation (**https://<IP address>/redfish/v1/JobService/Jobs**) with payload mentioning the schedule details in the body.

i. To schedule scanning Now (immediately)

```
{
    "Payload":{
        "TargetUri":
        "/redfish/v1/Systems/System.Embedded.1/Bios/Actions/Oem/DellBios.RunBIOSLiveScanning"
    }
}
```

ii. To schedule scanning Daily

```
{
    "Payload":{
        "TargetUri":
        "/redfish/v1/Systems/System.Embedded.1/Bios/Actions/Oem/DellBios.RunBIOSLiveScanning"
    },
    "Schedule": {
        "RecurrenceInterval": "P1D"
    }
}
```

iii. To schedule scanning Monthly

```
{
    "Payload":{
        "TargetUri":
        "/redfish/v1/Systems/System.Embedded.1/Bios/Actions/Oem/DellBios.RunBIOSLiveScanning"
    },
    "Schedule": {
      "EnabledDaysOfMonth":[24]     (Day of the date from which you prefer to schedule monthly)
    }
}
```

iv. To schedule scanning Yearly

```
{
    "Payload":{
        "TargetUri":
        "/redfish/v1/Systems/System.Embedded.1/Bios/Actions/Oem/DellBios.RunBIOSLiveScanning"
    },
    "Schedule": {
                                    "RecurrenceInterval": "P365D"
    }
}
```

For more details about the systems and iDRAC releases, see the following links:

PowerEdge systems product support site www.dell.com/poweredgemanuals

iDRAC product manuals support site	www.dell.com/idracmanuals
iDRAC support site	www.dell.com/support/idrac

Note: Dell Technologies recommends updating the iDRAC firmware and other firmware such as BIOS, network card, and so on, to the latest versions. Updating the firmware provides the security benefits that are described in this white paper.

3 Conclusion

Maintaining the highest levels of server security is a given in the world today. With advances in technology, malicious activities are advancing, too, and they pose a great challenge to system security. iDRAC9 4.10.10.10 and higher checks BIOS integrity and offers regular BIOS live scanning. The iDRAC9 ensures that host BIOS booting is secure on select new PowerEdge Intel and AMD iDRAC9 systems.

- The major advantage of iDRAC9 and Intel Boot Guard is that a BIOS image can be recovered if it is corrupted.
- RoT of the host ensures a safe boot process where any tampering with the host BIOS is identified early and mitigated.
- Having a recurring verification process for a BIOS image as the host is operating ensures protection from possible security threats.
- BIOS image integrity scanning mechanism on schedule basis enhances customer awareness when BIOS is compromised even when host is running.
- Good alerting mechanism when scanning fails using LED indication and logging an event.
- Potential damage from malicious software can be prevented right at boot.

A Troubleshooting

1. When customer logs in to an iDRAC, a SEL event is found mentioning that iDRAC has failed to verify BIOS, but host booted successfully.

    - This event is part of iDRAC HW RoT, even after a failed BIOS image verification, iDRAC performs a recovery operation to bring good BIOS image.

2. Host is booted to operating system, but the host has no network access to due to a timeout.

    - When BMC does not come up to perform HW RoT, the system is built with mechanism to detect this condition. The system then performs a safe boot for the host.

3. The BIOS booting fails due to BIOS image integrity check failure, and the subsequent BIOS recovery fails. Use the following mechanism can be used to recover the BIOS manually.

    - Upload the BIOS DUP from any of the iDRAC interfaces (for example: iDRAC UI).
    - Perform the racadm BIOS recover command as mentioned in Section 2 of this document.

B Glossary

Component	Description
BIOS	Basic Input/ Output System, also known as the System BIOS, ROM BIOS
FCH	Fusion Controller Hub
iDRAC	Integrated Dell Remote Access Controller
LED	Light Emitting Diode, is a semiconductor light source that emits light when current flows through it.
ME	Intel Management Engine
OS	Operating System
PCH	Platform Controller Hub - It controls certain data paths and support functions that are used with Intel CPUs.
POST	Power-On Self-Test
ROM	Read Only Memory
RoT	Root of Trust
UEFI	Unified Extensible Firmware Interface

C Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell Technologies storage platforms.

C.1 Related resources

Document Name (Document Link)	Document Description
https://github.com/corna/me_cleaner/wiki/Intel-Boot-Guard	Intel Boot Guard
https://edk2-docs.gitbooks.io/understanding-the-uefi-secure-boot-chain/secure_boot_chain_in_uefi/intel_boot_guard.html	Understanding the UEFI Secure Boot Chain - Intel® Boot Guard
https://2016.zeronights.ru/wp-content/uploads/2017/03/Intel-BootGuard.pdf	Safeguarding rootkits: Intel BootGuard
http://www.uefi.org/specifications	UEFI Specification
https://downloads.dell.com/solutions/dell-management-solution-resources/Secure%20Boot%20Management%20On%20DellEMC%20PowerEdge%20Servers.pdf	Secure Boot Management on DELL EMC PowerEdge Servers.
https://blog.dellemc.com/en-us/hardware-root-trust/	What Is Hardware Root of Trust?