iDRAC9 System Lockdown: Preventing Unintended Server Changes

Tech Note by

Kim Kinahan
Doug Iler
Rick Hall
Marshal Savage

Summary

Enabling system lockdown mode is part of Dell Technologies' cyber resilient architecture of Protect, Detect and Recover.

System Lockdown helps prevent change or "drift" in system firmware images and critical server configuration settings.

Dell Technologies is the only vendor to offer the ability to dynamically enable and disable system lockdown once your server is provisioned and in production without having to reboot.

Introduction

Running the latest firmware on datacenter servers helps keep up with security and performance improvements, maintain optimal operating parameters, and leverage new features. All are critical to the bottom line, to getting the most from your datacenter investment.

When unplanned or unforeseen changes occur to server configurations, whether benign or malicious, these can propagate across a datacenter with a corresponding loss in productivity or extra cost.

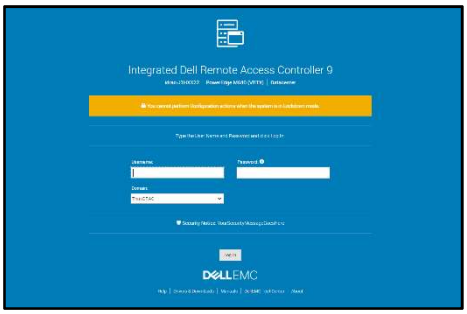
iDRAC9 System Lockdown Benefits

To prevent unintentional changes, the iDRAC9 Enterprise and Datacenter licenses now include a feature "System Lockdown," a virtual lock for firmware and hardware configurations. Even those with full admin privileges are limited to read-only access—unless the lock is first disabled. This prevents server 'drift', the unintentional migration of firmware and configuration settings across servers.

The lock does, however, allow for continued access to key operations, such as power capping and power cycling, health monitoring and virtual console access, while keeping server workloads running. All hypervisor and OS functionality are also fully accessible.

When accessed via a web GUI, Redfish REST APIs, or RACADM command-line utility, systems administrators are prevented from making changes that could impact servers in production. Additionally, the lockdown status is evident via a padlock icon and greyed out settings in the iDRAC GUI.

Even before logging in, the admin is notified the system is in Lockdown mode.



iDRAC9 System Lockdown is Part of Dell's Cyber Resilient Architecture

The lockdown mode is part of Dell's PowerEdge cyber resilient architecture, with its emphasis on Protect, Detect and Recover. It protects by preventing firmware downgrades as a possible vector of attack, adding or removing users as a means of circumventing settings, or modifying lockout policies. System Lockdown enables detecting changes outside a maintenance window by creating alerts in the iDRAC lifecycle log that can be configured to send notifications, and it potentially cuts recovery time spent re-imaging or re-configuring servers.

System lockdown now offers native lockdown support in select NICs which prevents malware in the OS from installing firmware updates using altered versions of vendor tools. This also addresses concerns for cloud providers of end customers installing their own firmware versions on the server hardware they are using. As a result, subsequent users of a cloud server can be assured that the networking adaptor firmware is secure and version consistent.

System Lockdown Drives Datacenter Efficiencies

The system lockdown fits well with standard server maintenance window methodologies, the unlocking and locking of servers serving as 'bookends' at the start or end of maintenance work. Once operationalized, it helps drive good maintenance behavior, cuts unforced errors, and prevent server 'drift'.

In Conclusion

Enabled in iDRAC Enterprise and Datacenter licenses, the lockdown feature is another important tool available from Dell Technologies to manage and maximize your investment in your PowerEdge servers.

PowerEdge DfD Repository
For more technical learning

Contact Us
For feedback and requests

Follow Us
For PowerEdge news