Server and Infrastructure Engineering

Direct from Development

Improved iDRAC9 Security using TLS 1.3 over HTTPS on Dell PowerEdge Servers

Tech Note by

Doug Iler
Aniruddha Herekar
Kim Kinahan

Summary

The iDRAC is designed for secure local and remote server management and offers industry-leading security features.

iDRAC9 5.10.00.00 supports TLS 1.3 over HTTPS, to encrypt data and authenticate connections for moving data over the internet.

TLS 1.3 uses advanced encryption algorithms, fewer cipher suites, and more secure handshakes.

Features supported by iDRAC9 over HTTPS using TLS 1.3 include:

- iDRAC9 Web Server
- Firmware Updates
- Export SupportAssist
- Import/Export Server Configuration File
- Export Inventory
- Export Lifecycle Log

Introduction

Data Center Managers rely on remote server management to deploy, update, and monitor their servers to extend their reach without having physical access to them. Securing your remote connection with encryption and secure login credentials is one way to prevent malicious actors from gaining access to your server. A secure connection prevents the deletion of critical data, ability to apply malware, or alter the system configuration.

Embedded within every Dell PowerEdge server is a powerful leading-edge remote server management processor, the Integrated Dell Remote Access Controller (iDRAC). The iDRAC is designed for secure local and remote server management and offers industry-leading security features. iDRAC9 establishes an encrypted connection over HTTPS using an SSL/TLS certificate to authenticate to web browsers and command line utilities. iDRAC9 version 5.10.00.00, now supports TLS v1.3 over HTTPS.

Secure communications with SSL/TLS

The iDRAC Web User Interface can be reached with any supported browser. iDRAC uses an SSL/TLS certificate to authenticate itself to web browsers and command line utilities, establishing an encrypted link. Transport Layer Security (TLS) is one of the most widely used security protocols.

When a user goes to a website, their browser checks for a TLS certificate on the site. If a certificate is present, their browser performs a TLS handshake to check its validity and authenticate the server. Once a link has been established between the two servers, TLS encryption and SSL decryption enable secure data transport.

There are several options available to secure the network connection using an TLS/SSL certificate. iDRACs web server has a self-signed TLS/SSL certificate by default. The self-signed certificate can be replaced with a custom certificate, a custom signing certificate, or a certificate signed by a well-known Certificate Authority (CA). Automated certificate upload can be accomplished by using Redfish scripts. The iDRAC9 Automatic Certificate Enrollment and Renewal feature automatically assures SSL/TLS certificates are in place and up to date for both bare-metal and previously installed systems. The Automatic Certificate Enrollment and Renewal feature requires the iDRAC9 Datacenter license.

TLS 1.3

TLS 1.3 offers several advantages over TLS 1.2. TLS version 1.3 uses advanced encryption algorithms, fewer cipher suites and, faster and more secure handshakes. Enabling TLS 1.3 results in better network connection performance.

Many new operating systems and browsers support TLS 1.3. Web browsers and command-line utilities, such as RACADM and WS-Man, use this TLS/SSL certificate for server authentication and to establish an encrypted connection. If the HTTPS server is configured for TLS 1.3, the clients will automatically detect it and perform the operation over TLS 1.3.

iDRAC9 Web Server can be configured with options to support “TLS 1.3 only.” Use the “TLS 1.3 only” option when the HTTPS client can support it. Older browsers that do not support TLS 1.3 should be configures to “TLS 1.2 and Higher” or “TLS 1.1 and Higher.”

Once iDRAC is configured and the TLS/SSL certificate is installed on the management stations, SSL enabled clients can access iDRAC securely and without certificate warnings.

Conclusion

iDRAC9 continues to support that latest security standards to meet the needs of security focused customers. iDRAC9 5.10.00.00 TLS 1.3 support over HTTPS, enables you to use the most current security stance for remotely managing your PowerEdge servers.

PowerEdge DfD Repository
For more technical learning

Contact Us
For feedback and requests

Follow Us
For PowerEdge news