Improved security of iDRAC9 with Lifecycle Controller via SMB2 Protocol

Maintaining best in class security of Dell EMC PowerEdge Servers

Abstract

This technical white paper provides detailed information about SMB2 Protocol support in iDRAC with Lifecycle controller.

October 2018

Revisions

Date	Description
October 2018	Initial release

Acknowledgements

This paper was produced by the following members of the Dell EMC storage engineering team:

Authors:

- Aniruddha Herekar
- Doug Iler
- Murali Somarothu

Table of contents

Revisions....2
Acknowledgements....2
Executive summary & Commonly Used Terms....4
1 Introduction....5
2 Advantages of SMB2 over CIFS/ SMB1....6
3 Dell-EMC SMB2 Client support....8
4 Conclusion....10
A Glossary....11
B Technical support and resources....12
B.1 Related references/ resources....12

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. With the latest firmware release of iDRAC with Lifecycle Controller, support for CIFS/SMBv1 is deprecated and is replaced with SMB Protocol 2 support. SMB2 includes SMBv2 and SMBv3 and, in this document, the term SMB2 referred to both. The updated protocol provides more secure connections and flexibility for future improvements.

This document provides some of the security aspects that are enhanced with SMB2.

Commonly used terms

Commonly used terms in this document:

- iDRAC – Integrated Dell Remote Access Controller
- CIFS – Common Internet File System
- SMB – Server Message Block

For a list of more terms, see Glossary.

1 Introduction

In 2017, there was a cyberattack by a crypto ransomware worm named WannaCry. This worm targeted systems with Microsoft Windows OS. WannaCry encrypted the files on the target computers and demanded ransom to decrypt them. The vulnerability that WannaCry exploits lies in the Windows implementation of the CIFS/SMBv1 protocol. Exploiting this protocol, the WannaCry ransomware pushed specifically crafted executable messages on the targets and execute code to encrypt the files. Though Microsoft released a patch for it, WannaCry infected many systems because the patch was not applied in time.

Because iDRAC includes additional security checks, it was not impacted by the WannaCry attack. However, as a security enhancement, Dell EMC is deprecating the CIFS/ SMBv1 protocol. Going forward, only the SMB2 protocol is supported. With this change, users need to have network shares with SMB2 protocol support when using iDRAC. Although SMBv1/CIFS protocol can still be kept enabled on the shares, it is not recommended.

2 Advantages of SMB2 over CIFS/SMB1

SMB2 protocol provides better security and durability. Following are advantages of SMB2 over CIFS and a summary of the changes in each version of SMB.

SMB version	Change history
SMB 1.0	Initial release of SMB.
SMB 2.0 First major redesign of SMB	• Increased file sharing scalability • Improved performance – Request compounding – Asynchronous operations – Larger reads/writes • More secure and robust – Small command set – Signing now uses HMAC SHA-256 instead of MD5 – SMB2 durability
SMB 2.1	• File leasing improvements • Large MTU support • BranchCache
SMB 3.0	• Availability – SMB Transparent Failover – SMB Witness – SMB Multichannel • Performance – SMB Scale-Out – SMB Direct (SMB 3.0 over RDMA) – SMB Multichannel – Directory Leasing – BranchCache V2 • Backup – VSS for Remote File Shares • Security – SMB Encryption using AES-CCM (Optional) – Signing now uses AES-CMAC • Management – SMB PowerShell – Improved performance counters – Improved Eventing
SMB 3.02	• Automatic rebalancing of Scale-Out File Server clients • Improved performance of SMB Direct (SMB over RDMA) • Support for multiple SMB instances on a Scale-Out File Server.

For more information about SMB and the versions, see the following Microsoft blog: https://blogs.technet.microsoft.com/josebda/2013/10/02/windows-server-2012-r2-which-version-of-the-smb-protocol-smb-1-0-smb-2-0-smb-2-1-smb-3-0-or-smb-3-02-are-you-using

More details about the features listed earlier are as follows:

- Password encryption and authentication is improved by using the stronger HMAC-MD5 algorithm (NTLMv2) compares to the previous DES algorithm (LAN Manager).
- Reduced Commands – There are 19 commands, which reduces complexity of the protocol implementation and exposure to attacks.
- Improved message signing and signing is per user. HMAC SHA-256 is used instead of MD5 as the hashing algorithm.
- Larger reads and writes better utilize faster networks even with high latency.
- Improved scalability for file sharing; the number of users, shares, and open files per server is increased.
- Durable handles - Allows a stateful connection to be reestablished if there are network issues.
- SMB2 allows client-side caching of folder and file properties.
- Compounding requests - Allows multiple requests to be sent in a single packet. This method is also called pipelining.
- Supports SMB direct (SMBv3 over RDMA), which improves performance.
- SMBv3 uses AES-CMAC message signing, which is more secure.
- SMBv3 allows optional encryptions of packets using AES-CCM encryption standard.

3 Dell-EMC SMB2 client support

The support for CIFS/SMBv1 protocol has changed in recent releases of iDRAC with Lifecycle Controller. While these changes are not visible to the end user, they remediate known issues of CIFS/SMBv1 protocol. CIFS/SMBv1 reportedly have security flaws that an attacker can exploit to execute rouge code by sending specially crafted messages to a SMBv1 server.

The releases starting which iDRAC with LC supports SMB2 protocol are listed in the table.

The versions marked as **No** for SMBv2 support CIFS/SMBv1.

PowerEdge server generation	iDRAC version	iDRAC supports SMBv2	LC UI supports SMBv2
12th and 13th generations	2.52.52.52	Yes	No
12th and 13th generations	2.60.60.60	Yes	Yes
14th generation	3.00.00.00	No	No
14th generation	3.02.00.01 - 3.21.21.21	Yes	No

In 14th generation, SMBv2 support in LC UI will be added in an upcoming iDRAC release targeted at Q1 CY2019.

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

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

iDRAC with LC performs additional security checks and supports some of the required features of SMB2 with a few simple measures. While some dialects (versions) and features are currently not supported, they will be supported in future releases.

iDRAC SMBv2 client supports the following features:

- Supports SMB 2.1 (0x210) dialect only.
- Supports NTLMv2 protocol for authentication.
- Supports both 56-bit and 128-bit encryption.
- Supports message signing.

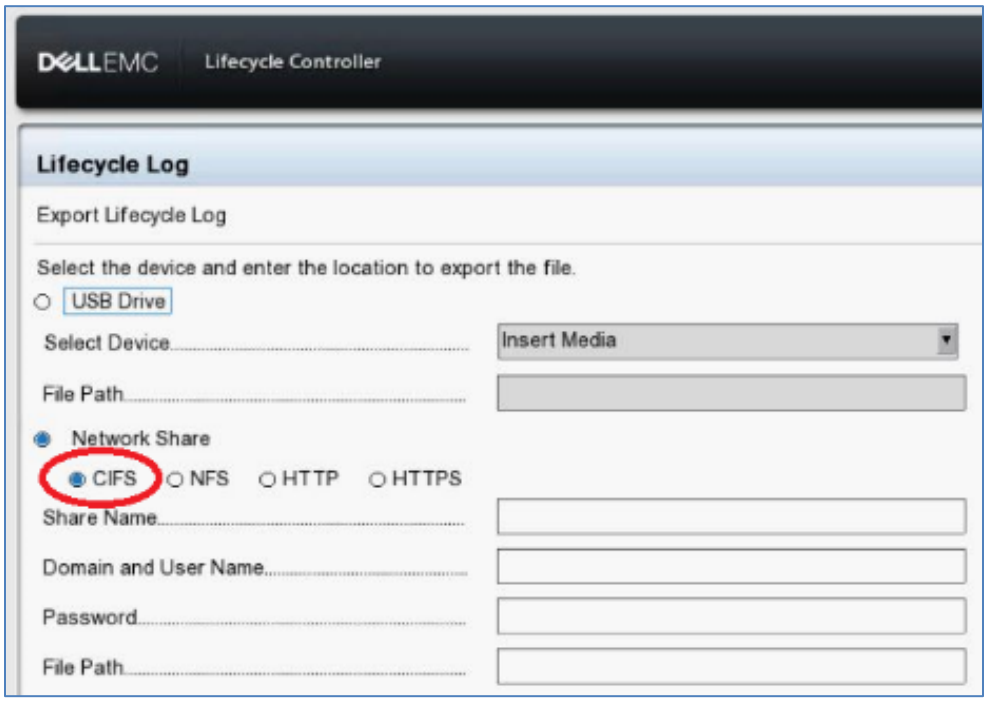
LC UI SMBv2 client supports the following features:

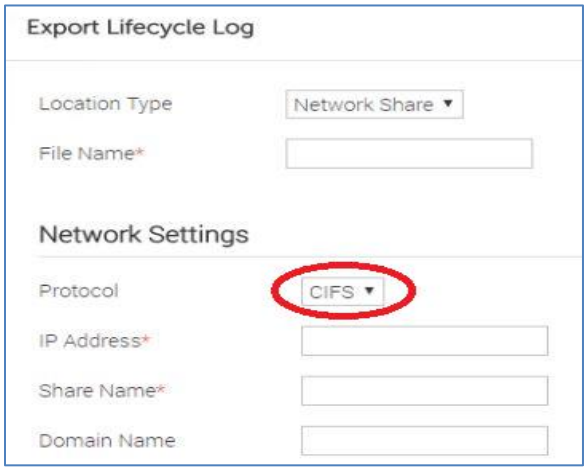
- Supports SMB 2.0.2 (0x202) and SMB 2.1 (0x210) dialects.
- Supports NTLMv2 protocol for authentication.
- Supports only 128-bit encryption as part of NTLMv2.

Note: Message signing is not supported in current releases. However, limited data intake, such as DUP file as input, which is validated at different steps, reduces the need for message signing in this pre-boot UEFI application.

At the time of writing this white paper. no SMBv3 protocol or dialects are supported.

Even though CIFS protocol is replaced with SMB2 protocol at the backend, the interfaces (iDRAC and LC GUI) still display the name **CIFS**. Example are shown in the following images.





Note: Dell EMC recommends updating the iDRAC firmware and other firmware such as BIOS, network card, and so on, to latest versions. Updating the firmware provides the security benefits of SMB2 protocol.

4 Conclusion

SMBv2 protocol has replaced the older CIFS/SMBv1 protocol. SMBv2 protects against security threats and provides the benefits of other security measures.

Dell EMC is committed to improve security measures and provide the users with secure products. We will be improving the security measures in SMB2 and other protocols in future releases. We recommend that users check the *New and enhanced features* section in the Release Notes for iDRAC releases for details of enhancements.

A Glossary

Component	Description
AES-CCM	Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code
AES-CMAC	Advanced Encryption Standard- Cipher-based Message Authentication Code
CIFS	Common Internet File System
DES	The Data Encryption Standard is a symmetric-key algorithm for the encryption of electronic data.
DUP	Dell Update Package - Firmware update executable file.
GUI	Graphical User Interface
HMAC-MD5	HMAC-MD5 is a type of keyed hash cryptographic algorithm that is constructed from the Message Digest Algorithm 5 (MD5) hash function and used as a Hash-based Message Authentication Code (HMAC).
HMAC SHA-256	HMAC SHA-256 is a type of keyed hash cryptographic algorithm that is constructed from the Secure Hash Algorithm 3 - 256 bits (SHA-256) hash function and used as a Hash-based Message Authentication Code (HMAC).
iDRAC	Integrated Dell Remote Access Controller
LAN Manager	LAN (Local Area Network) Manager is a network operating system originally co-developed by IBM and Microsoft.
LC GUI	Lifecycle Controller Graphical User Interface
LC UI	Lifecycle Controller User Interface
NTLMSSP	NT LAN Manager (NTLM) Security Support Provider is a binary messaging protocol used by the Microsoft Security Support Provider Interface (SSPI) to facilitate NTLM challenge-response authentication and to negotiate integrity and confidentiality options.
OS	Operating System
RFC	A Request for Comments (RFC) is a type of publication from the Internet Engineering Task Force (IETF) and the Internet Society (ISOC), the principal technical development and standards-setting bodies for the Internet.
SMB	Server Message Block
TCP	Transmission Control Protocol
UEFI	Unified Extensible Firmware Interface specification

B Technical support and resources

The Dell EMC Support website is focused on meeting customer needs with proven services and support.

The Dell EMC Knowledge Base is an online technical community where IT professionals have access to numerous resources for Dell EMC software, hardware and services. This link takes you directly to the iDRAC page.

B.1 Related references/ resources

Document Name (Document Link)	Document Description
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack	WannaCry ransomware attack Wiki page
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/	Blog with details about why you should stop using SMBv1.
https://msdn.microsoft.com/en-us/library/cc246482.aspx	[MS-SMB2]: Server Message Block (SMB) Protocol Versions 2 and 3
https://msdn.microsoft.com/en-us/library/cc236621.aspx	[MS-NLMP]: NT LAN Manager (NTLM) Authentication Protocol
https://blogs.technet.microsoft.com/josebda/2013/10/02/windows-server-2012-r2-which-version-of-the-smb-protocol-smb-1-0-smb-2-0-smb-2-1-smb-3-0-or-smb-3-02-are-you-using/	Blog about features of various SMB versions.
https://richardkok.wordpress.com/2011/02/03/wireshark-determining-a-smb-and-ntlm-version-in-a-windows-environment/	Wireshark: Determining a SMB and NTLM version in a Windows environment
https://support.microsoft.com/en-in/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and	How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server
http://www.uefi.org/specifications	UEFI Specification