Using Server Message Block (SMB) in iDRAC9 of Dell EMC PowerEdge Servers

This Dell EMC technical white paper describes the use of SMB in iDRAC9 of 14th generation Dell EMC PowerEdge servers.

Dell EMC Server Solutions
September 2017

Authors

Murali Somarouthu

Prashanth Giri

A Dell EMC Technical White Paper

Revisions

Date	Description
September 2017	Initial release

Contents

Executive summary

This technical white paper is aimed at the customers using iDRAC9's file sharing service by using the Server Message Block (SMB) protocol. Starting from the 14th generation of Dell EMC PowerEdge servers, iDRAC9 uses SMB 2.0 as the minimum SMB protocol version.

Document type definitions (DTDs) and required content

The Server Message Block (SMB) protocol is a network file sharing (NFS) protocol used by clients to access remote files or other services at remote server over network. Starting from iDRAC9, to provide increased security on the iDRACs when using network shares, the default minimum SMB version supported is now 2.1, instead of 1.0. The SMB 1.0 version reportedly has security flaws that an attacker can exploit to execute rogue code by sending specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server. Microsoft recommends using higher protocol versions of the SMB which are more secure in lieu of version 1.0.

SMB versions

SMB in iDRAC9

Starting from iDRAC9, the default minimum SMB protocol version is 2.1, which communicates by using the SMB 2.0 protocol with SMB server. The SMB2 protocol support was added to Windows Vista, Windows Server 2008, and later versions. By following best practice recommended for SMB shares, customers can disable SMBv1 and enable SMB 2.0 protocol to ensure that the shares are using secured protocol.

SMB/CIFS/SMB1	• Designed at IBM and tweaked by Microsoft in 1990, this is the first of SMB protocols that provided network file share early on. It is very inefficient and unsecured.
SMB 2.0	• Introduced by Microsoft with Windows Vista in 2006, this protocol reduced chattiness and supports message signing with SHA-256 hashing algorithm, and has better scalability. • Supported by Samba 3.6 or later. Durable file handle support added in Samba 4.0.
SMB 2.1	• Introduced in Windows 7 and Windows Server 2008 R2, with minor performance enhancements. • Supported by Samba 4.0 but leases feature was added in 4.2.
SMB 3.0	• Previously known as SMB 2.2, was introduced with Windows 8 and Windows Server 2012. Has several improvements including multiple connections per SMB session, transparent failure, and several security enhancements including end to end encryption with AES 128 CCM encryption. • Supported by Samba 4.0.0.
SMB 3.0.2	• Introduced with Windows 8.1 and Windows Server 2012 R2, provided an option to disable the unsecured SMBv1 to help provide increased security. • Support not provided by Samba servers.
SMB 3.1.1	• Introduced with Windows 10 and Windows Server 2016, this version supports AES128 GCM encryption and implements pre-authentication integrity check by using SHA-512 hash. It also makes secure negotiation mandatory when connecting clients by using the SMB 2.x or later versions. • Support not provided by Samba servers.

1 Comparison matrix showing SMB versions supported on different Microsoft Operating Systems (OSs).

OS	Windows 10 WS* 2016 TP2	Windows 8.1 WS* 2012 R2	Windows 8 WS* 2012	Windows 7 WS* 2008 R2	Windows Vista WS* 2008	Previous versions
Windows 10 WS* 2016 TP2	SMB 3.1.1	SMB 3.0.2	SMB 3.0	SMB 2.1	SMB 2.0.2	SMB 1.x
Windows 8.1 WS* 2012 R2	SMB 3.0.2	SMB 3.0.2	SMB 3.0	SMB 2.1	SMB 2.0.2	SMB 1.x
Windows 8 WS* 2012	SMB 3.0	SMB 3.0	SMB 3.0	SMB 2.1	SMB 2.0.2	SMB 1.x
Windows 7 WS* 2008 R2	SMB 2.1	SMB 2.1	SMB 2.1	SMB 2.1	SMB 2.0.2	SMB 1.x
Windows Vista WS* 2008	SMB 2.0.2	SMB 2.0.2	SMB 2.0.2	SMB 2.0.2	SMB 2.0.2	SMB 1.x
Previous versions	SMB 1.x	SMB 1.x	SMB 1.x	SMB 1.x	SMB 1.x	SMB 1.x

1.1 SBMv1 vulnerabilities

In early summer 2017, Microsoft released a security bulletin, MS17-010, advising about patching the vulnerable Windows versions to fix a serious vulnerability in the SMBv1 server. The most severe of the vulnerabilities could allow running a remote code, if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server. The vulnerability was exploited in one of the large ransomware campaign that has been observed since Friday, May 12th, 2017. The payload delivered is a variant of ransomware malware called WannaCry.

The immediate mitigation efforts to protect against such attacks were to patch the vulnerable Windows versions, disabling SMBv1 and switching to latest versions of SMB that are more secure and efficient.

1.2 SMB support in iDRAC versions

Traditionally iDRAC has supported SMB versions that were current with the release. Several previous generations of iDRACs have supported SMBv1 shares. Support for latest versions of SMB protocol are generally added as they become available over the iDRAC generations. Below table summarizes the different versions supported by the DRACs over different generations.

iDRAC version	iDRAC8 and below	iDRAC9 Windows share	iDRAC9 Samba share
Protocol Support	SMB 1.x	SMB 2.x SMB 3.0 SMB 3.0.2	SMB 2.x SMB 3.0

Starting from iDRAC9, the default minimum SMB protocol version is 2.1, which communicates by using the SMB 2.0 protocol with SMB server. The SMB2 protocol support was added to Windows Vista, Windows Server 2008, and later versions. By following best practice recommended for SMB shares, customers can disable SMBv1 and enable SMB 2.0 protocol to ensure that the shares are using secured protocol.

iDRAC9 can no longer mount shares that still uses SMBv1-only protocol. It is recommended to use SMB 2.0 or later versions of the protocol in the server to be able to use from iDRAC9.

1.3 Setting up SMB 2.0–based server

Windows 8 and Windows Server 2012

- To get the current state of the SMB server protocol configuration, run the following cmdlet:
  ```
  Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol
  ```
  - ```
    EnableSMB1Protocol  EnableSMB2Protocol
    ------------------  ------------------
    False                 True
    ```
- To disable SMBv1 on the SMB server, run the following cmdlet:
  ```
  Set-SmbServerConfiguration -EnableSMB1Protocol $false
  ```
- To disable SMBv2 and SMBv3 on the SMB server, run the following cmdlet:
  ```
  Set-SmbServerConfiguration -EnableSMB2Protocol $false
  ```
- To enable SMBv1 on the SMB server, run the following cmdlet:
  ```
  Set-SmbServerConfiguration -EnableSMB1Protocol $true
  ```
- To enable SMBv2 and SMBv3 on the SMB server, run the following cmdlet:
  ```
  Set-SmbServerConfiguration -EnableSMB2Protocol $true
  ```

Windows 7, Windows Server 2008 R2, Windows Vista, and Windows Server 2008

- To disable SMBv1 on the SMB server, run the following cmdlet:
  ```
  Set-ItemProperty -Path
  "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type
  DWORD -Value 0 -Force
  ```
- To disable SMBv2 and SMBv3 on the SMB server, run the following cmdlet:
  ```
  Set-ItemProperty -Path
  "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Type
  DWORD -Value 0 -Force
  ```
- To enable SMBv1 on the SMB server, run the following cmdlet:
  ```
  Set-ItemProperty -Path
  "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type
  DWORD -Value 1 -Force
  ```
- To enable SMBv2 and SMBv3 on the SMB server, run the following cmdlet:
  ```
  Set-ItemProperty -Path
  "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Type
  DWORD -Value 1 -Force
  ```

Note: You must restart the server after you make these changes.
  ```

1.4 Setting up SMB on the Linux OSs

1. Edit the Samba configuration file that is generally located at `/etc/samba/smb.conf`.
2. Add or edit the minimum and maximum protocol attributes to reflect the protocol version:

    - max protocol = SMB 2.0
    - min protocol = SMB 2.0
3. Restart the Samba server (by using the `root` credentials).

Technical support and resources

- Dell.com/support is focused on meeting customer requirements with proven services and support.
- Dell TechCenter is an online technical community where IT professionals have access to numerous resources for Dell EMC software, hardware, and services.
- Storage Solutions Technical Documents on Dell TechCenter provides expertise that enables you to ensure customer success on Dell EMC Storage platforms.
- How to enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server.