[MS-SMB2]: Server Message Block (SMB) Protocol Versions 2 and 3

This topic lists the Errata found in [MS-SMB2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata below are for Protocol Document Version V56.0 – 2018/09/12.

Errata Published*	Description
2018/12/17	In Section 2.2.2.2.2.1, MOVE_DST_IPADDR structure, the description of the (IPv4Address/Reserved2)/ IPv6Address (16 bytes) field has been changed from: (IPv4Address/Reserved2)/ IPv6Address (16 bytes): This field is interpreted in different ways depending on the type of IP address passed in. Reserved2 (12 bytes): The client MUST set this to 0, and the server MUST ignore it on receipt. If the value of the Type field is MOVE_DST_IPADDR_V6, this field is the IPv6Address field. Changed to: (IPv4Address/Reserved2)/ IPv6Address (16 bytes): This field is interpreted in different ways depending on the value of the Type field. Reserved2 (12 bytes): The server MUST set this to 0, and the client MUST ignore it on receipt. If the value of the Type field is MOVE_DST_IPADDR_V6, this field is the IPv6Address field. In Section 3.3.5.7, Receiving an SMB2 TREE_CONNECT Request, the following has been changed from: If TreeConnect.Share.Type includes STYPE_CLUSTER_SOFS, Connection.Dialect is "3.1.1" and the SMB2_TREE_CONNECT_FLAG_REDIRECT_TO_OWNER bit is set in the Flags field of the SMB2 TREE_CONNECT request, the server MUST query the underlying object store in an implementation-specific manner to determine whether the share is hosted on this node. If not, the server MUST return error data as specified in section 2.2.2 with ErrorData set to SMB2 ERROR Context response formatted as ErrorId set to SMB2_ERROR_ID_SHARE_REDIRECT, and ErrorContextData set to the Share Redirect error context data as specified in section 2.2.2.2.2 with IPAddrMoveList set to the list of IP addresses obtained in an implementation-specific manner. Changed to: If TreeConnect.Share.Type includes STYPE_CLUSTER_SOFS, Connection.Dialect is "3.1.1" and the SMB2_TREE_CONNECT_FLAG_REDIRECT_TO_OWNER bit is set in the Flags field of the SMB2 TREE_CONNECT request, the server MUST query the underlying object store in an implementation-specific manner to determine whether the share is hosted on this node. If not, the server MUST fail the tree connect request by setting the Status field in SMB2 header to

Errata Published*	Description
	STATUS_BAD_NETWORK_NAME, return error data as specified in section 2.2.2 with ErrorData set to SMB2 ERROR Context response formatted as ErrorId set to SMB2_ERROR_ID_SHARE_REDIRECT, and ErrorContextData set to the Share Redirect error context data as specified in section 2.2.2.2.2 with IPAddrMoveList set to the list of IP addresses determined for where to access the share. In this same section, changed from: If Connection.Dialect is "3.0.2" or "3.1.1" and TreeConnect.Share.Type includes STYPE_CLUSTER_SOFS, the server SHOULD<239> set the SMB2_SHARE_CAP_ASYMMETRIC bit in the Capabilities field in an implementation specific manner. If Connection.Dialect is "3.1.1" and TreeConnect.Share.SupportsIdentityRemoting is set, the server MUST set the SMB2_SHAREFLAG_IDENTITY_REMOTING bit in the ShareFlags field of the SMB2 TREE_CONNECT response. If Connection.Dialect is "3.1.1", TreeConnect.Share.Type includes STYPE_CLUSTER_SOFS, and the SMB2_TREE_CONNECT_FLAG_REDIRECT_TO_OWNER bit is set in the Flags field of the SMB2 TREE_CONNECT request, the server MUST fail the tree connect request with a STATUS_BAD_NETWORK_NAME error, set the ErrorId in the SMB2 Error Context response to SMB2_ERROR_ID_SHARE_REDIRECT, and return an error context response, as specified in section 2.2.2.2.2, with IPAddrMoveList set to the list of IP addresses obtained in a implementation-specific manner. <239> Section 3.3.5.7: Windows Server 2012 R2 also verifies whether TreeConnect.Share is asymmetric before setting the SMB2_SHARE_CAP_ASYMMETRIC bit in Changed to: If Connection.Dialect is "3.0.2" or "3.1.1", TreeConnect.Share.Type includes STYPE_CLUSTER_SOFS, and TreeConnect.Share is asymmetric, the server MUST set the SMB2_SHARE_CAP_ASYMMETRIC bit in the Capabilities field. If Connection.Dialect is "3.1.1" and TreeConnect.Share.SupportsIdentityRemoting is set, the server MUST set the SMB2_SHAREFLAG_IDENTITY_REMOTING bit in the ShareFlags field of the SMB2 TREE_CONNECT response. If Connection.Dialect is "3.1.1", TreeConnect.Share.Type includes STYPE_CLUSTER_SOFS, and the SMB2_TREE_CONNECT_FLAG_REDIRECT_TO_OWNER bit is set in the Flags field of the SMB2 TREE_CONNECT request and the SMB2_SHARE_CAP_ASYMMETRIC bit is set in the Capabilities field, the server SHOULD<239> set the SMB2_SHARE_CAP_REDIRECT_TO_OWNER bit in the Capabilities field. <239> Section 3.3.5.7: Windows Server v1709 operating system and later and Windows Server 2019 and later support the SMB2_SHARE_CAP_REDIRECT_TO_OWNER bit.
2018/12/10	In Section 3.3.5.9.12, Handling the SMB2_CREATE_DURABLE_HANDLE_RECONNECT_V2 Create Context, the following has been changed from: The server MUST look up an existing Open in the GlobalOpenTable by doing a lookup with the FileId.Persistent portion of the create context. If the lookup fails, the server SHOULD<280> fail the request with STATUS_OBJECT_NAME_NOT_FOUND and proceed as specified in "Failed Open Handling" in section 3.3.5.9.

Errata Published*	Description
	<281> Section 3.3.5.9.12: Windows Server 2012 with [KB2770917] and Windows 8 with [KB2770917] fail the CREATE request with STATUS_INVALID_PARAMETER if the request includes the SMB2_DHANDLE_FLAG_PERSISTENT bit in the Flags field of the SMB2_CREATE_DURABLE_HANDLE_RECONNECT_V2 Create Context. If the Session was established by specifying PreviousSessionId in the SMB2 SESSION_SETUP request, therefore invalidating the previous session, Windows 8.1 and Windows Server 2012 R2 close the durable opens established on the previous session. Changed to: The server MUST look up an existing Open in the GlobalOpenTable by doing a lookup with the FileId.Persistent portion of the create context. If the lookup fails: If the request includes the SMB2_DHANDLE_FLAG_PERSISTENT bit in the Flags field of the SMB2_CREATE_DURABLE_HANDLE_RECONNECT_V2 create context, the server MUST look up an existing Open in the GlobalOpenTable by doing a lookup with the CreateGuid of the create context. If the lookup fails, the server SHOULD<281> fail the request with STATUS_OBJECT_NAME_NOT_FOUND and proceed as specified in "Failed Open Handling" in section 3.3.5.9. Otherwise, the server SHOULD<282> fail the request with STATUS_OBJECT_NAME_NOT_FOUND and proceed as specified in "Failed Open Handling" in section 3.3.5.9. <281> Section 3.3.5.9.12: Windows 8 with [KB2770917] and Windows Server 2012 with [KB2770917] fail the CREATE request with STATUS_INVALID_PARAMETER. <282> Section 3.3.5.9.12: If the Session was established by specifying PreviousSessionId in the SMB2 SESSION_SETUP request, therefore invalidating the previous session, Windows 8.1 and Windows Server 2012 R2 close the durable opens established on the previous session.
2018/12/10	In Section 3.2.5.5, Receiving an SMB2 TREE_CONNECT Response, the following has been changed from: If Connection.Dialect is "3.1.1", the Status field in the SMB2 header of the response is STATUS_BAD_NETWORK_NAME, and the ErrorId in the SMB2 Error Context response is set to SMB2_ERROR_ID_SHARE_REDIRECT, the client MUST return the Share Redirect Error Context response to the calling application as specified in section 2.2.2.2.2. Changed to: If Connection.Dialect is "3.1.1", SMB2_TREE_CONNECT_FLAG_REDIRECT_TO_OWNER bit is set in the Flags field of the SMB2 TREE_CONNECT Request, the Status field in the SMB2 header of the response is STATUS_BAD_NETWORK_NAME, and the ErrorId in the SMB2 Error Context response is set to SMB2_ERROR_ID_SHARE_REDIRECT, the client MUST return the Share Redirect Error Context response to the calling application as specified in section 2.2.2.2.2.
2018/11/12	In Section 2.2.37, SMB2 QUERY_INFO Request, the following has been added to the list under FileInfoClass: • FileIdInformation In Section 3.3.5.20.1, Handling SMB2_0_INFO_FILE, the following was added:

Errata Published*	Description
	If the server does not implement the SMB 3.x dialect family and the request is for the FileIdInformation information class, the server MUST fail the request with STATUS_NOT_SUPPORTED.
2018/10/29	In Section 2.2.31, SMB2 IOCTL Request, the following has been changed from: Buffer (variable): A variable-length buffer that contains the input and output data buffer for the request, as described by the InputOffset, InputCount, OutputOffset, and OutputCount. There is no minimum size restriction for this field as there can be FSCTLs with no input or output buffers. For FSCTL_SRV_COPYCHUNK or FSCTL_SRV_COPYCHUNK_WRITE, the format of this buffer is specified in SRV_COPYCHUNK_COPY. The Buffer format for FSCTL_DFS_GET_REFERRALS is specified in [MS-DFSC] section 2.2.2. The format of this buffer for all other FSCTLs is specified in the reference topic for the FSCTL being called. Changed to: Buffer (variable): A variable-length buffer that contains the input and output data buffer for the request, as described by the InputOffset, InputCount, OutputOffset, and OutputCount. There is no minimum size restriction for this field as there can be FSCTLs with no input or output buffers. The format of this buffer for FSCTLs is specified in subsequent sections of 3.2.4.20. In Section 3.2.4.20.2.2, Application Requests a Server Side Data Copy, the following has been changed from: The SMB2 IOCTL Request MUST be initialized as follows: ● The CtlCode field MUST be set to the FSCTL code supplied by the application. ● The FileId field is set to Open.FileId. ● The InputOffset field is set to the offset to the Buffer[], in bytes, from the beginning of the SMB2 header. ● The InputCount is set to the size, in bytes, of the SRV_COPYCHUNK_COPY structure that is constructed following the syntax specified in section 2.2.31.1.1 with the client input parameters as follows: ● The client sets the SourceKey field to the key of the source file. ● For each range to be copied, the client initializes a SRV_COPYCHUNK structure following the syntax specified in section 2.2.31.1.1 using the provided source offset, destination offset, and length, in bytes. ● The ChunkCount is set to the number of chunks being sent. ● The SRV_COPYCHUNK_COPY structure is copied into the request at InputOffset bytes from the beginning of the SMB2 header. ● The OutputOffset field SHOULD<125> be set to zero. ● The OutputCount field is set to 0. ● The MaxInputResponse field is set to 0. ● The MaxOutputResponse field is set to the size of a SRV_COPYCHUNK_RESPONSE structure, as specified in section 2.2.32.1. ● SMB2_0_IOCTL_IS_FSCTL is set to TRUE in the Flags field. The request MUST be sent to the server. Changed to: The SMB2 IOCTL Request MUST be initialized as follows: ● The CtlCode field MUST be set to the FSCTL code supplied by the application. ● The FileId field is set to Open.FileId.

Errata Published*	Description
	• The Buffer field is set to an SRV_COPYCHUNK_COPY Request, as specified in section 2.2.31.1. • The SourceKey field is set to the key of the source file. • For each range to be copied, the client initializes the Chunks field following the syntax specified in section 2.2.31.1.1 using the application provided source offset, destination offset, and length, in bytes. • The ChunkCount is set to the number of chunks being sent. • The InputOffset field is set to the offset to the Buffer, in bytes, from the beginning of the SMB2 header. • The InputCount is set to the size, in bytes, of the Buffer field. • The OutputOffset field SHOULD<125> be set to zero. • The OutputCount field is set to 0. • The MaxInputResponse field is set to 0. • The MaxOutputResponse field is set to the size of a SRV_COPYCHUNK_RESPONSE structure, as specified in section 2.2.32.1. • SMB2_0_IOCTL_IS_FSCTL is set to TRUE in the Flags field. The request MUST be sent to the server. In Section 3.2.4.20.3, Application Requests DFS Referral Information, the following has been changed from: The application provides the following: • ServerName: The name of the server from which to query referrals. • UserCredentials: An opaque implementation-specific entity that identifies the credentials to be used when authenticating to the remote server. • The maximum output buffer response size, in bytes. • An input buffer containing the application-provided REQ_GET_DFS_REFERRAL or REQ_GET_DFS_REFERRAL_EX structure. • FSCTL code. Changed to: The application provides the following: • ServerName: The name of the server from which to query referrals. • UserCredentials: An opaque implementation-specific entity that identifies the credentials to be used when authenticating to the remote server. • The maximum output buffer response size, in bytes. • An input buffer containing the application-provided structure REQ_GET_DFS_REFERRAL specified in [MS-DFSC] section 2.2.2 or REQ_GET_DFS_REFERRAL_EX specified in [MS-DFSC] section 2.2.3. • The FSCTL code for DFS referral information, either FSCTL_DFS_GET_REFERRALS or FSCTL_DFS_GET_REFERRALS_EX. In Section 3.2.4.20.7, Application Requests Content Information for a File, the following has been changed from: The SMB2 IOCTL Request MUST be initialized as follows: • The CtlCode field is set to FSCTL_SRV_READ_HASH. • The FileId field is set to Open.FileId. • The InputOffset field is set to the offset to the Buffer[], in bytes, from the beginning of the SMB2 header.

Errata Published*	Description
	• The InputCount is set to the size, in bytes, of the SRV_READ_HASH request structure that is constructed following the syntax specified in section 2.2.31.2 with the client input parameters as follows: • The client initializes a SRV_READ_HASH request structure following the syntax specified in section 2.2.31.2 using the applicationprovided hash type, hash version, hash retrieval type, length and offset, in bytes. • The SRV_READ_HASH request structure is copied into the request at InputOffset bytes from the beginning of the SMB2 header. • The OutputOffset field SHOULD<132> be set to zero. • The OutputCount field is set to 0. • The MaxInputResponse field is set to 0. • The MaxOutputResponse field is set to the maximum number of bytes that the application expects to retrieve. • The SMB2_0_IOCTL_IS_FSCTL in the Flags field is set to TRUE. The request MUST be sent to the server, and the response from the server MUST be handled as described in section 3.2.5.14.7. The status of the response MUST be returned to the application. Changed to: The SMB2 IOCTL Request MUST be initialized as follows: • The CtlCode field is set to FSCTL_SRV_READ_HASH. • The FileId field is set to Open.FileId. • The Buffer field is set to an SRV_READ_HASH Request, as specified in section 2.2.31.2. • The client initializes an SRV_READ_HASH request structure following the syntax specified in section 2.2.31.2 using the application-provided hash type, hash version, hash retrieval type, length, and offset, in bytes. • The InputOffset field is set to the offset to the Buffer, in bytes, from the beginning of the SMB2 header. • The InputCount is set to the size, in bytes, of the Buffer field. • The OutputOffset field SHOULD<132> be set to zero. • The OutputCount field is set to 0. • The MaxInputResponse field is set to 0. • The MaxOutputResponse field is set to the maximum number of bytes that the application expects to retrieve. • The SMB2_0_IOCTL_IS_FSCTL in the Flags field is set to TRUE. The request MUST be sent to the server, and the response from the server MUST be handled as described in section 3.2.5.14.7. The status of the response MUST be returned to the application. In Section 3.2.4.20.8, Application Requests Resiliency on an Open File, the following has been changed from: The SMB2 IOCTL Request MUST be initialized as follows: • The CtlCode field MUST be set to FSCTL_LMR_REQUEST_RESILIENCY. • The FileId field MUST be set to Open.FileId. • The InputOffset field MUST be set to the offset to the Buffer[], in bytes, from the beginning of the SMB2 header. • The InputCount field MUST be set to the size, in bytes, of the NETWORK_RESILIENCY_REQUEST structure specified in section 2.2.31.3. • A NETWORK_RESILIENCY_REQUEST structure MUST be appended to the request at InputOffset bytes from the beginning of the SMB2 header. The Timeout field of

Errata Published*	Description
	the NETWORK_RESILIENCY_REQUEST structure MUST be set to the time-out (in milliseconds) provided by the application. • The OutputOffset field SHOULD<133> be set to zero. • The OutputCount field MUST be set to 0. • The MaxInputResponse field MUST be set to 0. • The MaxOutputResponse field MUST be set to 0. • SMB2_0_IOCTL_IS_FSCTL in the Flags field MUST be set to TRUE. The request MUST be sent to the server, and the response from the server MUST be handled as described in section 3.2.5.14.9. The status of the response MUST be returned to the application. Changed to: The SMB2 IOCTL Request MUST be initialized as follows: • The CtlCode field MUST be set to FSCTL_LMR_REQUEST_RESILIENCY. • The FileId field MUST be set to Open.FileId. • The Buffer field is set to a NETWORK_RESILIENCY_REQUEST Request, as specified in section 2.2.31.3. • The Timeout field MUST be set to the application-provided time-out (in milliseconds). • The InputOffset field MUST be set to the offset to the Buffer, in bytes, from the beginning of the SMB2 header. • The InputCount field MUST be set to the size, in bytes, of the Buffer field. • The OutputOffset field SHOULD<133> be set to zero. • The OutputCount field MUST be set to 0. • The MaxInputResponse field MUST be set to 0. • The MaxOutputResponse field MUST be set to 0. • SMB2_0_IOCTL_IS_FSCTL in the Flags field MUST be set to TRUE. The request MUST be sent to the server, and the response from the server MUST be handled as described in section 3.2.5.14.9. The status of the response MUST be returned to the application.
2018/10/29	In Section 3.3.5.9, Receiving an SMB2 CREATE Request, the following has been changed from: If Connection.Dialect belongs to the SMB 3.x dialect family and the request does not contain SMB2_CREATE_DURABLE_HANDLE_RECONNECT Create Context or SMB2_CREATE_DURABLE_HANDLE_RECONNECT_V2 Create Context, the server MUST look up an existing open in the GlobalOpenTable where Open.FileName matches the file name in the Buffer field of the request. If an Open entry is found, and if all the following conditions are satisfied, the server MUST fail the request with STATUS_FILE_NOT_AVAILABLE. • Open.IsPersistent is TRUE • Open.Connection is NULL • Open.OplockLevel is not equal to SMB2_OPLOCK_LEVEL_BATCH Open.OplockLevel is not equal to SMB2_OPLOCK_LEVEL_LEASE or Open.Lease.LeaseState does not include SMB2_LEASE_HANDLE_CACHING Changed to: If Connection.Dialect belongs to the SMB 3.x dialect family and the request does not contain SMB2_CREATE_DURABLE_HANDLE_RECONNECT Create Context or

Errata Published*	Description
	SMB2_CREATE_DURABLE_HANDLE_RECONNECT_V2 Create Context, the server MUST look up an existing open in the GlobalOpenTable where Open.FileName matches the file name in the Buffer field of the request. If an Open entry is found, and if all the following conditions are satisfied, the server SHOULD<240> fail the request with STATUS_FILE_NOT_AVAILABLE. ● Open.IsPersistent is TRUE ● Open.Connection is NULL <240> Section 3.3.5.9: If Open.ClientGuid is not equal to the ClientGuid of the connection that received this request, Open.Lease.LeaseState is equal to RWH or Open.OplockLevel is equal to SMB2_OPLOCK_LEVEL_BATCH, Windows-based servers will attempt to break the lease/oplock and return STATUS_PENDING to process the create request asynchronously. Otherwise, if Open.Lease.LeaseState does not include SMB2_LEASE_HANDLE_CACHING and Open.OplockLevel is not equal to SMB2_OPLOCK_LEVEL_BATCH, Windows-based servers return STATUS_FILE_NOT_AVAILABLE.
2018/10/29	In Section 2.2.13.2.13, SMB2_CREATE_APP_INSTANCE_ID, the description of the StructureSize field has been changed from: StructureSize (2 bytes): The client MUST set this field to 20 , indicating the size of this structure. Changed to: StructureSize (2 bytes): This field MUST be set to 20 , indicating the size of this structure. In Section 2.2.13.2.15, SMB2_CREATE_APP_INSTANCE_VERSION, the description of the StructureSize field has been changed from: StructureSize (2 bytes): The client MUST set this field to 24, indicating the size of this structure. Changed to: StructureSize (2 bytes): This field MUST be set to 24, indicating the size of this structure. In Section 3.3.5.9.13, Handling the SMB2_CREATE_APP_INSTANCE_ID and SMB2_CREATE_APP_INSTANCE_VERSION Create Contexts, the following has been added: The server MAY validate the StructureSize field of the create context.
2018/10/29	In Section 3.2.5.19.3, Receiving an Oplock Break Acknowledgment Response, the following has been changed from: If the client receives success in the response, no further processing is required. If the client receives an error in the response to the Oplock Break Acknowledgment, the client MUST set Open.OplockLevel to SMB2_OPLOCK_LEVEL_NONE. Changed to:

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>If the Status field in the SMB2 header of the response to the Oplock Break Acknowledgment is zero, no further processing is required.
Otherwise, the client MUST set Open.OplockLevel to SMB2_OPLOCK_LEVEL_NONE.

In Section 3.2.5.19.4, Receiving a Lease Break Acknowledgment Response, the following has been changed from:

No processing is required for this response.

Changed to:

If the Status field in the SMB2 header of the response to the Lease Break Acknowledgment is zero, no further processing is required.
Otherwise, the client MUST set File.LeaseState to SMB2_LEASE_NONE and Open.OplockLevel to SMB2_OPLOCK_LEVEL_NONE.</td></tr>
<tr><td>2018/09/17</td><td>In Section 2.2.13, SMB2 CREATE Request, in the list of values for the CreateOptions field, the description for the FILE_NO_INTERMEDIATE_BUFFERING value has been corrected (a key change is that a missing "not" has been added to the condition).

Changed from:

CreateOptions (4 bytes): Specifies the options to be applied when creating or opening the file. Combinations of the bit positions listed below are valid, unless otherwise noted. This field MUST be constructed using the following values.<31>

<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>…</td><td>…</td></tr><tr><td>FILE_NO_INTERMEDIATE_BUFFERING
0x00000008</td><td>File buffering is not performed on this open; file data is retained in memory before writing or after reading it from the underlying storage.</td></tr><tr><td>…</td><td>…</td></tr></table>
Changed to:

CreateOptions (4 bytes): Specifies the options to be applied when creating or opening the file. Combinations of the bit positions listed below are valid, unless otherwise noted. This field MUST be constructed using the following values.<31>

<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>…</td><td>…</td></tr><tr><td>FILE_NO_INTERMEDIATE_BUFFERING
0x00000008</td><td>File buffering is not performed on this open; file data is not retained in memory upon writing it to, or reading it from, the underlying storage.</td></tr><tr><td>…</td><td>…</td></tr></table></td></tr>
</table>

*Date format: YYYY/MM/DD