[MS-FSRVP]: File Server Remote VSS Protocol

This topic lists the Errata found in the MS-FSRVP document 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 V8.0 – 2015/06/30.

Errata Published*	Description
2015/08/03	In Section 3.1.4, Message Processing Events and Sequencing Rules, clarified which security measures the server must enforce in order to verify that the caller has the required permissions to execute any method. Changed from: The server SHOULD<4> enforce security measures to verify that the caller has the required permissions to execute any method. If the server enforces security measures, and the caller does not have the required credentials, then the server MUST fail the call and return E_ACCESSDENIED. For more details on how to determine the identity of the caller for the purpose of performing an access check, see [MS-RPCE] section 3.3.3.1.3. <4> Section 3.1.4: Windows servers check whether the caller is a member of the administrators or backup operators group. Changed to: The server MUST enforce the below security measures to verify that the caller has the required permissions to execute any method.<4>. ▪ The security provider as RPC_C_AUTHN_GSS_NEGOTIATE or RPC_C_AUTHN_GSS_KERBEROS or RPC_C_AUTHN_WINNT, as specified in [MS-RPCE] section 2.2.1.1.7. ▪ The authentication level as RPC_C_AUTHN_LEVEL_PKT_INTEGRITY or RPC_C_AUTHN_LEVEL_PKT_PRIVACY, as specified in [MS-RPCE] section 2.2.1.1.8.If the caller does not have the required permissions, then the server MUST fail the call and return E_ACCESSDENIED. For more details on how to determine the identity of the caller for the purpose of performing an access check, see [MS-RPCE] section 3.3.3.1.3. <4> Section 3.1.4: Windows servers additionally check whether the caller is a member of the administrators or backup operators group.
2015/07/20	In Section 2.2.2.1, SHADOW_COPY_ATTRIBUTES, ATTR_FILE_SHARE was removed from the table of valid values. In Section 2.2.2.2, CONTEXT_VALUES, the first paragraph was changed from: The context of a shadow copy is a combination of zero or more attribute values, as defined in section 2.2.2.1. The following table lists the valid context values for the shadow copy operations. The client can additionally include the ATTR_AUTO_RECOVERY attribute in any of the following contexts. Changed to: The context of a shadow copy is a combination of zero or more attribute values, as defined in section 2.2.2.1. The following table lists the valid context values for the shadow copy operations. The client can additionally include either the ATTR_AUTO_RECOVERY or ATTR_NO_AUTO_RECOVERY attribute in any of the following contexts.

*Date format: YYYY/MM/DD