OVAL Userright updates
January 20, 2016

1. Summary

The OVAL Windows *userright* test was added to OVAL 5.11 as recommended by SPAWAR. After developing code to utilize this test and creating test content SPAWAR realized that it needs to be updated for easier content development and results that are easier to understand by end users.

When SPAWAR proposed the test for 5.11, we originally had it defined to use *trustee_name*, but based on feedback from the OVAL community, we switched this to *trustee_sid*, however we should have allowed for either *trustee_name* or *trustee_sid*. Additionally, we are proposing updating both the *trustee_sid* and *trustee_name* to have *maxOccurs = 1*.

Adding *trustee_name* allows for much easier content development when the SID is unknown, which is frequently the case with applications such as SQL Server and/or IIS Server. Having the *trustee_name* as part of the object also makes the results easier to understand for end users. If just the *trustee_sid* is included, there's no easy way for the end user to know the correlation between some random *trustee_sid* and the text based *trustee_name,* which makes remediation more challenging.

Updating the *maxOccurs* from unbounded to 1 also helps make the results easier to understand, and is in alignment with how the fileeffectiverights53, registryeffectiveright53, fileaudited, registryauditedpermissions etc… are designed, and they all have the same trustee_name and trustee_sid elements.

2. New Capabilities that Cannot Currently be Accomplished with OVAL

This update allows for easier content development, especially when the content author needs to include a trustee, which does not have a well-known SID. See example content and results for details, and explained in detail in section 11 of this document.

3. Relevance of the New Capability

This update would be relevant to Windows only and only to content using OVAL 5.11 and later.

4. Impact upon OVAL Content Developers

This update makes *userright* content easier to write, especially for trustees without well-known SIDs.

5. Impact upon OVAL Content Consumers

OVAL content consumers that support the OVAL 5.11 *userright* test will need to have two minor updates.

1. Add the *trustee_name* to the object and state
2. Update *maxOccurs* on *trustee_name* and *trustee_sid* from unbounded to 1.

6. Impact upon Existing OVAL Content

None.

7. Impact upon Existing OVAL Implementations

Same as #5.

8. Relevance to Existing OVAL Use Cases

Application of the *userright* test/object/state most directly affects the Configuration Management OVAL use case.

9. Affected OVAL Schema Documents

- windows-definitions-schema.xsd
- windows-system-characteristics-schema.xsd

10. Backward Compatibility with Previous Versions

None.

11. Demonstration of the New Capabilities

The revised Windows userright OVAL capability has been demonstrated with a pre-release version of the SCAP Compliance Checker 4.1 and sample content and results are available for review; refer to "win-def_userright_proposed_updates_content_and_results.zip."

Please note that this section's content is more directed at content authors.

11.1. Notes Regarding Included Sample Userright OVAL Content

Both sample content files, "userright_test-oval_Prototype_ForForum.xml" and "userright_test-oval_Prototype_ForForum_SQLUpdate.xml", contain the following 5 definitions:

- Def 1: Back up files and directories (SE_BACKUP_NAME) privilege example using trustee_sid.
- Def 2: Back up files and directories (SE_BACKUP_NAME) privilege example using trustee_name.
- Def 3: Manage auditing and security log (SE_SECURITY_NAME) privilege example where the requirement is No One, in this case trustee_sid is used, however trustee_name could be used in its place in the test.
- Def 4: Deny logon as a service (SE_DENY_SERVICE_LOGON_NAME) privilege example which must have guests and users groups assigned. Note that having additional trustees will not result in a failure, since that is considered more secure for a deny user right.
- Def 5; Adjust memory quotas for a process (SE_INCREASE_QUOTA_NAME) is allowed to have SQL related accounts and IIS Appool entities in this example.
  - Note: Def 5 is modified in "userright_test-oval_Prototype_ForForum_SQLUpdate.xml" to report a pass on a test of a specific test IIS and SQL server in our test lab. The other definitions are identical in both content files.

11.1.1. Notes Regarding Definitions Defined in Example OVAL Content

- Def 1 and Def 2 are examples of defining user right content that allows two known groups. Def 1 shows how to do so with trustee_sid and Def 2 shows the same requirement but this time it uses trustee_name. The results will be the same but this is can show how the content author can define content.
- Def 1 and Def 2 both allow for “more restrictive” user right settings. In other words if one or both of defined trustee’s are found, that will not result in a failure. If a subset is found, again not result in a failure. If no one is assigned the user right (this would be most restrictive setting), a failure will not be reported. Please review provided content file to see how this was done.
- Def 3 is an example of a user right who’s requirement is no one. In this case, if there is one or more trustee assigned, a failure will be reported.
- Def 4 is an example of a deny user right. A deny user right must have trustee’s defined in content or a failure will be reported. If there are additional trustee’s this is considered more secure and will not result in a failure.
- Def 5 is an example of content that could be used on a SQL and IIS server. Note that since the trustee_sid is not a known value and different on each server, utilizing trustee_name is the way this content should be written. Again please review content to see how this was done.

11.2. Notes Regarding Example of SCC Results From OVAL Content

There are 4 examples. Note the final two are labeled 3a and 3b since they deal with a IIS and SQL server and utilize different OVAL content. For tests 1, 2 and 3a the content used is “userright_test-oval_Prototype_ForForum.xml”, which has just been documented. For test 3b, please refer to the sample content file: “userright_test-oval_Prototype_ForForum_SQLUpdate.xml.” This has a change to definition 5 documented above and can been seen in Example 3b defined below.

- Example 1: Reviewing compliant Windows 7 system. In this example a windows 7 system was reviewed. All 5 definitions, with their associated tests, passed. Please review Example Results\Example 1.

- Example 2: Reviewing the same Windows 7 system. However, the system was modified to show failures for Def 1 and Def 2. Note that in both cases the results show the trustee_sid and trustee_name even though content specified one or the other.

- Additional notes regarding Example 1 and 2: In both results you can see that Def 4 has a deny user right that has more trustees than required. A pass is reported since this is considered more restrictive.

- Example 3a: Designed to look at Def 5 regarding configuring user rights on an IIS server. A failure is due to one trustee (SQLServer2005MSSQLUser group) not being in OVAL content regular expression. Please see Example 3a results folder.

- Example 3b: Designed to look at Def 5 regarding configuring user rights on a SQL server. Using “userright_test-oval_Prototype_ForForum_SQLUpdate.xml” (also in the Example Content folder) to add the SQLServer2005MSSQLUser group. Def 5 passed with the updated content.