- Open Vulnerability and Assessment Language - Element Dictionary

- Schema: Unix System Characteristics
- Version: 5.2
- Release Date: 31 January 2007

The following is a description of the elements, types, and attributes that compose the UNIX specific system characteristic items found in Open Vulnerability and Assessment Language (OVAL). Each item is an extension of the standard item element defined in the Core System Characteristic Schema. Through extension, each item inherits a set of elements and attributes that are shared amongst all OVAL Items. Each item is described in detail and should provide the information necessary to understand what each element and attribute represents. This document is intended for developers and assumes some familiarity with XML. A high level description of the interaction between the different tests and their relationship to the Core System Characteristic Schema is not outlined here.

The OVAL Schema is maintained by The Mitre Corporation and developed by the public OVAL Community. For more information, including how to get involved in the project and how to submit change requests, please visit the OVAL website at http://oval.mitre.org.

< file_item >

The file item holds information about the individual files found on a system. Each file item contains path and filename information as well as its type, associated user and group ids, relevant dates, and the privialeges granted. It extends the standard ItemType as defined in the oval-system-characteristics schema and one should refer to the ItemType description for more information.

Child Elements	Type	MinOccurs	MaxOccurs
path	oval-sc:EntityItemStringType	0	1
filename	oval-sc:EntityItemStringType	0	1
type	oval-sc:EntityItemStringType	0	1
group_id	oval-sc:EntityItemStringType	0	1
user_id	oval-sc:EntityItemStringType	0	1
a_time	oval-sc:EntityItemStringType	0	1
c_time	oval-sc:EntityItemStringType	0	1
m_time	oval-sc:EntityItemStringType	0	1
size	oval-sc:EntityItemIntType	0	1
suid	oval-sc:EntityItemBoolType	0	1
sgid	oval-sc:EntityItemBoolType	0	1
sticky	oval-sc:EntityItemBoolType	0	1
uread	oval-sc:EntityItemBoolType	0	1
uwrite	oval-sc:EntityItemBoolType	0	1
uexec	oval-sc:EntityItemBoolType	0	1
gread	oval-sc:EntityItemBoolType	0	1

gwrite	oval-sc:EntityItemBoolType	0	1
gexec	oval-sc:EntityItemBoolType	0	1
oread	oval-sc:EntityItemBoolType	0	1
owrite	oval-sc:EntityItemBoolType	0	1
oexec	oval-sc:EntityItemBoolType	0	1

< inetd_item >

The inetd item holds information associated with different Internet services. It extends the standard ItemType as defined in the oval-system-characteristics schema and one should refer to the ItemType description for more information.

Child Elements	Type	MinOccurs	MaxOccurs
protocol	oval-sc:EntityItemStringType	0	1
service_name	oval-sc:EntityItemStringType	0	1
server_program	oval-sc:EntityItemStringType	0	1
server_arguments	oval-sc:EntityItemStringType	0	1
endpoint_type	unix-sc:EntityEndpointType	0	1
exec_as_user	oval-sc:EntityItemStringType	0	1
wait_status	unix-sc:EntityWaitStatusType	0	1

< interface_item >

The interface item holds information about the interfaces on a system. Each interface item contains name and address information as well as any associated flags. It extends the standard ItemType as defined in the oval-system-characteristics schema and one should refer to the ItemType description for more information.

Child Elements	Type	MinOccurs	MaxOccurs
name	oval-sc:EntityItemStringType	0	1
hardware_addr	oval-sc:EntityItemStringType	0	1
inet_addr	oval-sc:EntityItemStringType	0	1
broadcast_addr	oval-sc:EntityItemStringType	0	1
netmask	oval-sc:EntityItemStringType	0	1
flag	oval-sc:EntityItemStringType	0	unbounded

< password_item >

/etc/passwd. See passwd(4).

Child Elements	Type	MinOccurs	MaxOccurs
username	oval-sc:EntityItemStringType	0	1
password	oval-sc:EntityItemStringType	0	1
user_id	oval-sc:EntityItemStringType	0	1
group_id	oval-sc:EntityItemStringType	0	1
gcos	oval-sc:EntityItemStringType	0	1
home_dir	oval-sc:EntityItemStringType	0	1
login_shell	oval-sc:EntityItemStringType	0	1

< process_item >

Output of /usr/bin/ps. See ps(1).

Child Elements	Type	MinOccurs	MaxOccurs
command	oval-sc:EntityItemStringType	0	1
exec_time	oval-sc:EntityItemStringType	0	1
pid	oval-sc:EntityItemIntType	0	1
ppid	oval-sc:EntityItemIntType	0	1
priority	oval-sc:EntityItemStringType	0	1
scheduling_class	oval-sc:EntityItemStringType	0	1
start_time	oval-sc:EntityItemStringType	0	1
tty	oval-sc:EntityItemStringType	0	1
user_id	oval-sc:EntityItemStringType	0	1

< runlevel_item >

The runlevel item holds information about the start or kill state of a specified service at a given runlevel. Each runlevel item contains service_name and runlevel information as well as start and kill information. It extends the standard ItemType as defined in the oval-system-characteristics schema and one should refer to the ItemType description for more information.

Child Elements	Type	MinOccurs	MaxOccurs
service_name	oval-sc:EntityItemStringType	0	1

runlevel	oval-sc:EntityItemStringType	0	1
start	oval-sc:EntityItemBoolType	0	1
kill	oval-sc:EntityItemBoolType	0	1

< sccs_item >

Child Elements	Type	MinOccurs	MaxOccurs
path	oval-sc:EntityItemStringType	0	1
filename	oval-sc:EntityItemStringType	0	1
module_name	oval-sc:EntityItemIntType	0	1
module_type	oval-sc:EntityItemIntType	0	1
release	oval-sc:EntityItemStringType	0	1
level	oval-sc:EntityItemStringType	0	1
branch	oval-sc:EntityItemStringType	0	1
sequence	oval-sc:EntityItemStringType	0	1
what_string	oval-sc:EntityItemStringType	0	1

< shadow_item >

/etc/shadow. See shadow(4).

Child Elements	Type	MinOccurs	MaxOccurs
username	oval-sc:EntityItemStringType	0	1
password	oval-sc:EntityItemStringType	0	1
chg_lst	oval-sc:EntityItemStringType	0	1
chg_allow	oval-sc:EntityItemStringType	0	1
chg_req	oval-sc:EntityItemStringType	0	1
exp_warn	oval-sc:EntityItemStringType	0	1
exp_inact	oval-sc:EntityItemStringType	0	1
exp_date	oval-sc:EntityItemStringType	0	1
flag	oval-sc:EntityItemStringType	0	1

< uname_item >

Information about the hardware the machine is running on. This information is the parsed equivalent of uname -a.

Child Elements	Type	MinOccurs	MaxOccurs
machine_class	oval-sc:EntityItemStringType	0	1
node_name	oval-sc:EntityItemStringType	0	1
os_name	oval-sc:EntityItemStringType	0	1
os_release	oval-sc:EntityItemStringType	0	1
os_version	oval-sc:EntityItemStringType	0	1
processor_type	oval-sc:EntityItemStringType	0	1

< xinetd_item >

The xinetd item holds information associated with different Internet services. It extends the standard ItemType as defined in the oval-system-characteristics schema and one should refer to the ItemType description for more information.

Child Elements	Type	MinOccurs	MaxOccurs
protocol	oval-sc:EntityItemStringType	0	1
service_name	oval-sc:EntityItemStringType	0	1
flags	oval-sc:EntityItemStringType	0	1
no_access	oval-sc:EntityItemStringType	0	1
only_from	oval-sc:EntityItemStringType	0	1
port	oval-sc:EntityItemStringType	0	1
server	oval-sc:EntityItemStringType	0	1
server_arguments	oval-sc:EntityItemStringType	0	1
socket_type	oval-sc:EntityItemStringType	0	1
type	unix-sc:EntityXinetdTypeStatusType	0	1
user	oval-sc:EntityItemStringType	0	1
wait	oval-sc:EntityItemBoolType	0	1
disabled	oval-sc:EntityItemBoolType	0	1

== EntityEndpointType ==

The EntityEndpointType complex type restricts a string value to a specific set of values that describe endpoint types associated with an Internet service. The empty string is also allowed to support empty emlement associated with error conditions.

Value	Description

stream
dgram
raw
seqpacket
tli

== EntityXinetdTypeStatusType ==

The EntityXinetdTypeStatusType complex type restricts a string value to three values, either RPC, INTERNAL, or UNLISTED that specify the type of service registered in xinetd. The empty string is also allowed to support empty emlement associated with error conditions.

Value	Description
INTERNAL	The INTERNAL type is used to describe services like echo, chargen, and others whose functionality is supplied by xinetd itself.
RPC	The RPC type is used to describe services that use remote procedure call ala NFS.
UNLISTED	The UNLISTED type is used to describe services that aren't listed in /etc/protocols or /etc/rpc.

== EntityWaitStatusType ==

The EntityWaitStatusType complex type restricts a string value to two values, either wait or nowait, that specify whether the server that is invoked by inetd will take over the listening socket associated with the service, and whether once launched, inetd will wait for that server to exit, if ever, before it resumes listening for new service requests. The empty string is also allowed to support empty emlement associated with error conditions.

Value	Description
wait	
nowait	