Samurai

Library version:	RENAT 0.1.10
Library scope:	test suite
Named arguments:	supported

Introduction

A library provides functions to control Samurai application

The library utilize *Selenium2Library* and adds more functions to control Samurai application easily. Without other furthur mentions, all of the concepts of `user`, `user group` are Samurai concepts. By default, RENAT will try to connec to all Samurai nodes defined in active `local.yaml` at the beginning of the test and disconnect from them at the end of the test automatically. Usually user does not need to use `Connect All` and `Close` explicitly.

Currently, this module supposed that Samurai is used in Japanese locale. When Samurai module has error, it tried to make the last snapshot in `result/selenium-screenshot-x.png`. Checking this capture will help to understand the reason of the error.

Currently the module support Samurai 09/14/16

Some keywords of Samurai is using `xpath` to identify elements. See *Selenium2Library* for more details about xpath.

See WebApp for common keywords of web applications and how to configure the `local.yaml` file.

Selenium2Library keywords still could be used together within this library. See Selenium2Library for more details.

Shortcuts

Add Policy · **A**dd Policy Group · **A**dd User · **C**apture Screenshot · **C**hange Policy View Group · **C**lick All Elements · **C**lose · **C**lose All · **C**lose Window · **C**onnect · **C**onnect All · **D**elete Policy · **D**elete Policy Group · **D**elete User · **E**dit Mitigation Controller · **E**dit Policy · **G**et Mitigation List · **L**eft Menu · **L**ogin · **L**ogout · **M**ake Item Map · **R**econnect · **R**eset Capture Counter · **S**elect Items In Table · **S**elect Window · **S**et Ajax Wait · **S**et Capture Counter · **S**et Capture Format · **S**how Detail Mitigation · **S**how Policy Basic · **S**how Policy Detection · **S**how Policy Mitigation · **S**how Policy Mo · **S**how Policy Monitor · **S**tart Mitigation · **S**top Mitigation · **S**witch

Keywords

<table>
<tr><th>Keyword</th><th>Arguments</th><th>Documentation</th></tr>
<tr><td><b>Add Policy</b></td><td><i>**policy</i></td><td>
Adds a new Samurai policy

`policy` is a map containing the below information to create the new policy.

<table>
<tr><th>key</th><th>meaning</th><th>mandatory</th><th>sample</th></tr>
<tr><td>name</td><td>name of the policy</td><td>yes</td><td><i>test001</i></td></tr>
<tr><td>basic_alias</td><td>alias name of the policy</td><td></td><td><i>test001</i></td></tr>
<tr><td>basic_port_id</td><td>another alias</td><td></td><td></td></tr>
<tr><td>basic_facing</td><td><code>customer</code> or <code>backbone</code></td><td></td><td><i>customer</i></td></tr>
<tr><td>basic_intf_list</td><td>list of router and interface pair, separated by comma</td><td>yes</td><td><i>10.128.18.31:xe-0/0/0.1</i></td></tr>
<tr><td>basic_cidr_list</td><td>list of CIDR separate by comma</td><td></td><td></td></tr>
<tr><td>basic_option_filter</td><td>optinal filter</td><td></td><td></td></tr>
<tr><td>basic_direction</td><td>direction of the traffic (<code>incoming</code> or <code>outgoing</code>)</td><td></td><td><i>Incoming</i></td></tr>
<tr><td>traffic_enabled</td><td>Enable traffic monitoring or not</td><td>yes</td><td><i>${TRUE}</i> or <i>${FALSE}</i></td></tr>
<tr><td>detection_enabled</td><td>Enable detection or not</td><td>yes</td><td><i>${TRUE}</i> or <i>${FALSE}</i></td></tr>
<tr><td>mitigation_enabled</td><td>Enable Mitigation or not</td><td>yes</td><td><i>${TRUE}</i> or <i>${FALSE}</i></td></tr>
<tr><td>mitigation_zone_name</td><td>Name of the zone for mitigation</td><td></td><td><i>zone001</i></td></tr>
<tr><td>mitigation_zone_prefix</td><td>Prefixes that could mitigate</td><td></td><td><i>1.1.1.1/32</i></td></tr>
<tr><td>mitigation_thr_bps</td><td>Upper limit (bps)</td><td></td><td><i>800,000,000</i></td></tr>
<tr><td>mitigation_thr_pps</td><td>Upper limit (pps)</td><td></td><td><i>54,000,000</i></td></tr>
<tr><td>mitigation_auto_enabled</td><td>Enable automitgation or not</td><td></td><td><i>${TRUE}</i> or <i>${FALSE}</i></td></tr>
<tr><td>mitigation_auto_level</td><td>Automitgation level</td><td></td><td>0:overLow 1:overMedium 2:High</td></tr>
<tr><td>mitigation_auto_time</td><td>Automitigation detect attack time (min)</td><td></td><td>default is 15</td></tr>
<tr><td>mitigation_mo_enabled</td><td>Using Arbor TMS MO or not</td><td>yes</td><td><i>${TRUE}</i> or <i>${FALSE}</i></td></tr>
<tr><td>mitigation_auto_stop_enabled</td><td>Enable automitgation stop or not</td><td></td><td><i>${TRUE}</i> or <i>${FALSE}</i></td></tr>
<tr><td>mitigation_auto_stop_level</td><td>Automitgation level</td><td></td><td>0:overLow 2:High</td></tr>
<tr><td>mitigation_auto_stop_time</td><td>Automitigation stop detect attack time (min)</td><td></td><td>default is 15</td></tr>
<tr><td>mitigation_device_list</td><td>Devices used for TMS, separated by comma</td><td></td><td><i>ArborSP-A</i></td></tr>
<tr><td>mitigation_mo_name</td><td>MO name, separated by comma</td><td></td><td><i>OCN12(ALU)_LOOSE</i></td></tr>
<tr><td>mitigation_comm_list</td><td>commna separated peer/community list</td><td></td><td><i>1.10(180.0.1.10)/2914:666,1.11(180.0.1.11)/2914:777</i></td></tr>
<tr><td>nw_monitor_gre1</td><td>1st GRE address for NW monitor</td><td></td><td><i>210.0.1.1</i></td></tr>
<tr><td>nw_monitor_gre2</td><td>2nd GRE address for NW monitor</td><td></td><td><i>210.0.1.1</i></td></tr>
<tr><td>nw_monitor_ce1</td><td>1st CE address for NW monitor</td><td></td><td><i>210.0.1.2</i></td></tr>
<tr><td>nw_monitor_ce2</td><td>2nd CE address for NW monitor</td><td></td><td><i>210.0.1.2</i></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td>
<table>
<tr><td>nw_monitor_pe1</td><td>1st PE for NW monitor (list)</td><td></td><td><i>edge01hige-MX2020-15(118.23.176.244)</i></td></tr>
<tr><td>nw_monitor_pe2</td><td>2nd PE for NW monitor (list)</td><td></td><td><i>edge01hige-MX2020-15(118.23.176.244)</i></td></tr>
<tr><td>event_name</td><td>name of the message event to make</td><td></td><td><i>info1</i></td></tr>
<tr><td>event_addr</td><td>address to send the events</td><td></td><td><i>user@mail.com</i></td></tr>
<tr><td>view_group</td><td>user group that could view this policy, separated by comma</td><td>yes</td><td><i>SuperGroup,test_group_007</i></td></tr>
</table>
Example:
<table>
<tr><td>Samurai.<i>Switch</i></td><td>samurai-1</td><td></td></tr>
<tr><td>Samurai.<i>Add Policy</i></td><td>name=${POLICY_NAME}</td><td>basic_alias=${POLICY_NAME}</td></tr>
<tr><td>...</td><td>basic_facing=customer</td><td>basic_intf_list=10.128.18.31:xe-0/0/0.1</td></tr>
<tr><td>...</td><td>basic_cidr_list=1.1.1.0/24</td><td>basic_direction=incoming</td></tr>
<tr><td>...</td><td>traffic_enabled=${TRUE}</td><td></td></tr>
<tr><td>...</td><td>detection_enabled=${TRUE}</td><td></td></tr>
<tr><td>...</td><td>mitigation_zone_name=test_zone001</td><td>mitigation_zone_prefix=1.1.1.1/32</td></tr>
<tr><td>...</td><td>mitigation_device_list=ArborSP-A,ArborSP-B</td><td></td></tr>
<tr><td>...</td><td>mitigation_mo_enabled=${TRUE}</td><td></td></tr>
<tr><td>...</td><td>mitigation_mo_name=N000000012_LOOSE</td><td></td></tr>
<tr><td>...</td><td>mitigation_comm_list=1.10(180.0.1.10)/2914:666,1.11(180.0.1.11)/2914:777</td><td></td></tr>
<tr><td>...</td><td>event_name=test</td><td>event_addr=user@mail.com</td></tr>
<tr><td>...</td><td>view_group=SuperGroup</td><td></td></tr>
</table>
</td></tr>
<tr><td><b>Add Policy Group</b></td><td><i>group_name</i>, <i>policy_list=*</i>, <i>limit_bps=4000000000</i>, <i>limit_pps=2700000</i></td><td>Add a new policy group

<code>group_name</code> is the name of the new group. <code>policy_list</code> is a comma separated of existed policy that should be bound to this policy. An asterisk for this parameter (<code>*</code>) means <i>all of the existed policy</i>. <code>limit_bps</code> and <code>limit_pps</code> are the mitigation capacity threshold of this group.</td></tr>
<tr><td><b>Add User</b></td><td><i>group</i>, <i>**user_info</i></td><td>Adds user to the current group <code>user_info</code> is a dictionary contains user information that has following keys: <code>name</code>, <code>password</code>, <code>privilege</code> and <code>policy</code>

<code>privilege</code> is existed privilege that has been created (e.g: <i>system_admin</i>.

<code>policy</code> could be <code>*</code> for all current policies or a list of policy names that are binded to this user.

<code>group</code> is the user group. <code>Dot(.)</code> means current group

Examples:
<table>
<tr><td>Samurai.<i>Add User</i></td><td>OCNDDoS</td><td>name=user000</td><td>password=Test12345678</td></tr>
<tr><td>...</td><td>privilege=system_admin</td><td>policy=*</td><td></td></tr>
<tr><td>Samurai.<i>Add User</i></td><td>OCNDDoS</td><td>username=user001</td><td>password=Test12345678</td></tr>
<tr><td>...</td><td>privilege=system_admin</td><td>policy=OCN11,OCN12</td><td></td></tr>
</table>
</td></tr>
<tr><td><b>Capture Screenshot</b></td><td><i>filename=None</i>, <i>extra=</i></td><td>Captures the current screen to file

Using the internal counter for filename if <code>filename</code> is not specified. In this case, the filename is defined by a pre-set format. <i>Set Capture Format</i> could be used to change the current format.

An extra information will be add to the filename if <code>extra</code> is defined

Examples:
<table>
<tr><td>Samurai.<i>Capture Screenshot</i></td><td></td><td># samurai_0000000001.png</td></tr>
<tr><td>Samurai.<i>Capture Screenshot</i></td><td>extra=_list</td><td># samurai_0000000002_<i>list</i>.png</td></tr>
<tr><td>Arbor.<i>Capture Screenshot</i></td><td></td><td># arbor_0000000001.png</td></tr>
<tr><td>Arbor.<i>Capture Screenshot</i></td><td>extra=_xxx</td><td># arbor_0000000001_<i>xxx</i>.png</td></tr>
<tr><td>Samurai.<i>Capture Screenshot</i></td><td>filename=1111.png</td><td># 1111.png</td></tr>
</table>
</td></tr>
<tr><td><b>Change Policy View Group</b></td><td><i>name</i>, <i>*group_name</i></td><td>Changes the groups that could see this policy

<code>name</code> is the policy name. <code>group_name</code> is a list of policies

Example:
<table>
<tr><td>Samurai.<i>Change Policy View Group</i></td><td>super_admin</td><td>test_group001</td></tr>
</table>
</td></tr>
<tr><td><b>Click All Elements</b></td><td><i>xpath</i></td><td>Click all element in current page defined by <code>xpath</code>

Returns the number of elements that have been clicked</td></tr>
<tr><td><b>Close</b></td><td></td><td>Closes the current active browser</td></tr>
<tr><td><b>Close All</b></td><td></td><td>Closes all current opened applications</td></tr>
<tr><td><b>Close Window</b></td><td></td><td>Closes the current window</td></tr>
<tr><td><b>Connect</b></td><td><i>app</i>, <i>name</i></td><td>Opens a web browser and connects to application and assigns a <code>name</code>.

If not defined in <code>local.yaml</code> those following key will have defaut values:
<table>
<tr><td>browser</td><td>firefox</td><td>optional</td></tr>
<tr><td>login_url</td><td>/</td><td>optiona</td></tr>
<tr><td>proxy:</td><td></td><td>optional</td></tr>
<tr><td>http: 10.128.8.210:8080</td><td>optional</td><td></td></tr>
<tr><td>ssl: 10.128.8.210:8080</td><td>optional</td><td></td></tr>
<tr><td>socks: 10.128.8.210:8080</td><td>optional</td><td></td></tr>
<tr><td>profile_dir</td><td>./config/samurai.profile</td><td>optional</td></tr>
</table>
</td></tr>
<tr><td><b>Connect All</b></td><td></td><td>Connects to all applications defined in <code>local.yaml</code>

The name of the connection will be the same of the <i>webapp</i> name</td></tr>
</table>

<table>
<tr><td><b>Delete Policy</b></td><td><i>*policy_names</i></td><td>Deletes poilcies by their names

Returned the number of deleted users

<b>Notes:</b> If the policy does not exists, the system will not report any error.

Examples:
<table><tr><td>Samurai.<i>Delete Policy</i></td><td>test001</td><td>test002</td></tr></table></td></tr>
<tr><td><b>Delete Policy Group</b></td><td><i>*group_list</i></td><td>Deletes policy groups

See <i>Select Items In Table</i> for more detail about how to choose <i>group_list</i>

Returns the number of deleted policy groups Example:
<table><tr><td>Samurai.<i>Delete Policy Group</i></td><td>test_group001</td><td>test_group002</td></tr></table></td></tr>
<tr><td><b>Delete User</b></td><td><i>group</i>, <i>*user_list</i></td><td>Deletes user from the user group

group is the user group. And . means current group Returns the number of deleted users

Examples:
<table><tr><td>Samurai.<i>Delete User</i></td><td>SuperGroup</td><td>user001</td><td>user002</td></tr><tr><td>Samurai.<i>Delete User</i></td><td>.</td><td>user002</td><td></td></tr></table></td></tr>
<tr><td><b>Edit Mitigation Controller</b></td><td><i>controller</i>, <i>**config</i></td><td>Change the setting of the mitigation control
<ul><li>control: name of the mitigation controller</li><li>config: configuration need to be changed. Currently only tms_group is configurable with the following format: groupname1:action1,groupname2:action2. groupname is currently set TMS group name and action could be <i>click</i>,<i>check</i> or <i>uncheck</i>.</li></ul>Example:
<table><tr><td>Samurai.<i>Edit Mitigation Controller</i></td><td>controller=vSP-A</td><td>tms_group=Logical0_SOCN_IPv4:uncheck</td></tr></table></td></tr>
<tr><td><b>Edit Policy</b></td><td><i>**policy</i></td><td>Edits a Samurai policy

policy contains information about the policy. See <i>Add Policy</i> for more details about policy format</td></tr>
<tr><td><b>Get Mitigation List</b></td><td><i>status=実行中</i></td><td>Gets current mitigation list

Return current active mitgation name, ID and the number of them

Example:
<table><tr><td>${MITI} ${IDS} ${NUM}=</td><td>Samurai.<i>Get Mitigation List</i></td></tr></table></td></tr>
<tr><td><b>Left Menu</b></td><td><i>menu</i>, <i>locator=None</i>, <i>ignore_first_element=True</i></td><td>Chooses the left panel menu by its displayed name

When locater is not null, the keyword will return a list of text attribute of all elements specified by the locator. locator could be a xpath or a predefined string.

locator predefined strings are: MITIGATE_REALTIME, MITIGATE_LIST, DETECT_LIST

For example, a xpath //div[@id='infoareain2']/*//td[1]/a means the list of <i>link</i> of all elements in a 1st column of a table insides a div with id infoareain2.

Examples:
<table><tr><td>Samurai.<i>Left Menu</i></td><td>Traffic</td><td></td><td></td></tr><tr><td>Samurai.<i>Left Menu</i></td><td>Detection</td><td></td><td></td></tr><tr><td>Samurai.<i>Left Menu</i></td><td>ポリシー管理</td><td></td><td></td></tr><tr><td>@{LIST}=</td><td>Samurai.<i>Left Menu</i></td><td>Active Mitigation</td><td>//div[@id='infoareain2']/*//td[1]/a</td></tr></table></td></tr>
<tr><td><b>Login</b></td><td></td><td>Logs-in into the application

User and password is set by the template and authentication methods in the master files</td></tr>
<tr><td><b>Logout</b></td><td></td><td>Logs-out the current application, the browser remains</td></tr>
<tr><td><b>Make Item Map</b></td><td><i>xpath</i></td><td>Makes a item/webelement defined <i>xpath</i>

The map is a dictionary from <i>item</i> to the <i>WebElement</i> Items name found by xpath are used as keys</td></tr>
<tr><td><b>Reconnect</b></td><td></td><td>Reconnects to the server</td></tr>
<tr><td><b>Reset Capture Counter</b></td><td></td><td>Resets the counter of the screen capture</td></tr>
<tr><td><b>Select Items In Table</b></td><td><i>xpath</i>, <i>xpath2</i>, <i>*item_list</i></td><td>Checks items in Samurai table by xpath

xpath points to the column that used as key and xpath2 is the relative xpath contains the target column.

item_list is a list of item and its action that need to check. Item in the list could be a regular expresion with the format re:<regular expression>|action.

The default action for the item could be click`<i>(default),</i>`check or uncheck

The keyword is called with assuming that the table is already visible.

Returns the tupple of all items and selected items

<b>Note:</b> Non-width-space (\u200b) will be take care by the keyword.

<b>Note:</b> if the first item_list is * then the keywork will try to click a link named <i>すべてを選択</i>.</td></tr>
<tr><td><b>Select Window</b></td><td><i>title</i></td><td>Selects a window by its title</td></tr>
<tr><td><b>Set Ajax Wait</b></td><td><i>wait_time=2s</i></td><td>Set the ajax wait time</td></tr>
<tr><td><b>Set Capture Counter</b></td><td><i>value=0</i></td><td>Sets the counter of the screen capture to value</td></tr>
<tr><td><b>Set Capture Format</b></td><td><i>format</i></td><td>Sets the format for the screen capture file

The format does not include the default prefix .png The default format is <mod>_%010d. mod could be samurai or arbor</td></tr>
</table>

<table>
<tr><td></td><td></td><td>See https://docs.python.org/2/library/string.html#format-specification-mini-language for more details about the format string.
Examples:
<table><tr><td>Samurai.<i>Set Capture Format</i></td><td>${case}_%010d</td><td># ${case} is a predefined variable</td></tr></table></td></tr>
<tr><td><b>Show Detail Mitigation</b></td><td><i>id</i></td><td>Shows detail information of a mitigation</td></tr>
<tr><td><b>Show Policy Basic</b></td><td><i>policy_name</i></td><td>Makes the virtual browser show basic setting of the policy <i>name</i>.
A following Samurai.<i>Capture Screenshot</i> is necessary to capture the result.</td></tr>
<tr><td><b>Show Policy Detection</b></td><td><i>policy_name</i></td><td>Shows the detction pannel of <i>policy_name</i> policy</td></tr>
<tr><td><b>Show Policy Mitigation</b></td><td><i>policy_name</i></td><td>Make the virtual browser show the mitigation setting of a policy
A following Samurai.<i>Capture Screenshot</i> is necessary to capture the result.</td></tr>
<tr><td><b>Show Policy Mo</b></td><td><i>policy_name</i></td><td>Make the virtual browser show the MO setting of a policy
Automatically expand the MO section of other devices if necessary.
A following Samurai.<i>Capture Screenshot</i> is necessary to capture the result.</td></tr>
<tr><td><b>Show Policy Monitor</b></td><td><i>policy_name</i></td><td>Make a virtual browser show the mitigation setting of a policy
A following Samurai.<i>Capture Screenshot</i> is necessary to capture the result.</td></tr>
<tr><td><b>Start Mitigation</b></td><td><i>policy</i>, <i>prefix</i>, <i>comment=mitigation started by RENAT</i>, <i>device=None</i>, <i>force=False</i></td><td>Starts a mitigation with specific <code>prefix</code>
<code>device</code> is used for matching real device name configured by Samurai If <code>force</code> is <code>TRUE</code> then the keyword will fail if selected device does not contain <code>device</code>
Returns mitigation <code>id</code> and selected <code>arbor device</code>
Example:
<table><tr><td>${id}</td><td>${device}=</td><td>Samurai.<i>Start Mitigation</i></td><td>211.1.12.1/32</td><td>mitigation by RENAT</td><td>SP-A</td><td>${TRUE}</td></tr></table></td></tr>
<tr><td><b>Stop Mitigation</b></td><td><i>id</i>, <i>stop_when_error=True</i></td><td>Stops a mitigation by its ID
Example:
<table><tr><td>Samurai.<i>Stop Mitigation</i></td><td>700</td></tr></table></td></tr>
<tr><td><b>Switch</b></td><td><i>name</i></td><td>Switches the current browser to <code>name</code></td></tr>
</table>

Altogether 37 keywords.
Generated by Libdoc on 2018-10-08 19:18:09.