How to write custom actions triggered both by the local agent as well as a central point with the ability to use Nimsoft to manage and report on these actions which may include scripting.

nexec probe: (command execution probe, local system or remote)

Description: run command anywhere -> on any machine and from any system

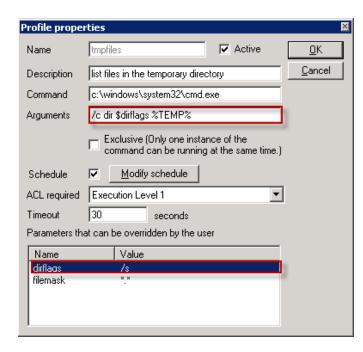
Features:

- Control what person or group is allowed to run the command
- Schedule a command to be run via nexec profile(s)
- Parameters: if you want to use a generic command, e.g., dir, you can set parameters to use in the command execution, for example:

Parameter Name Value dirflags /s

then call it in the command using \$dirflag

	🎆 nexec: [/Nimsoft-Demo/WorldWideHQ/apollo/nexec] 📃 🔀								
Ĺ	Setup		Configure	Start)			
Г	All profiles								
	Name	Command		Arguments	Exclusive	Schedule		Ī	
	🗹 interface info	ipconfig		/all	yes				
	🗹 test	cmd.exe			yes				
	test2	/bin/sh		-c ls /tmp/\$filemask					
	🗹 tmpfiles	c:\windows\system	32\cmd.exe	/c dir \$dirflags %TEMP%		DTSTART:20071221T1000	000 RRULE:FREQ=MINUTELY;INTERVAL=2 DTEND:20071222T100000		
	1								
	<u>O</u> K <u>C</u> ano	el <u>Apply</u>					<u><u>H</u>ei</u>	þ	



To test the command you can Select the Start Tab and then select the profile you created to execute the command, then rt-click it and Run it. You can then see the output as well as any errors if there's a problem, e.g., cant find a dir/file, bad command syntax, etc.

Infrastructure Manager Ne View Security Tools Window Help			
	•		
nexec: [/Nimsoft-Demo/WorldWideHQ/apollo/n	ехес]	_ 🗆 2	
Setup C	onfigure Start		
Profiles	Run profile		
Name Description	Run prome		
interface info test tmpfiles list files in the temporary directory	Name Impfiles Description list files in the temporary directory	_ <u>Close</u> 	
	Parameters that can be set by the user	_	
	Name Value dirflags /s filemask **		
Mersion 1.02. Started May 04 06:38:27 <u>OK</u> <u>Cancel</u> <u>Apply</u> <u>B</u> Be as400	Bun Done Done Std. Volume in drive C has no label.		
	05/04/2010 06:40 AM 0 axis2-tmp-19183063341604922228.tmp.lck 04/23/2010 04:59 PM OIR> axis2-tmp-292801605341804922228.tmp.lck 02/22/2010 02:37 AM OIR> axis2-tmp-2908769743207110987.tmp.lck 02/22/2010 12:37 AM OIR> axis2-tmp-2908769743207110987.tmp.lck 02/19/2010 05:42 PM OIR> axis2-tmp-3116314331905134151.tmp.lck 02/19/2010 05:42 PM OIR> axis2-tmp-3116314331905134151.tmp.lck 02/23/2010 03:54 PM OIR> axis2-tmp-3116314351905134151.tmp.lck 02/23/2010 03:54 PM OIR> axis2-tmp-3116324524756495.tmp.lck 04/10/2010 06:59 PM OIR> axis2-tmp-3436714082640208045.tmp		
	Std.		

Note: You can also select the nexec probe and press Ctrl-P, to interact directly with the probe to make a request and list the profiles or run one of the profiles to see the output. Note that you have to enter the name of the profile you want to run.

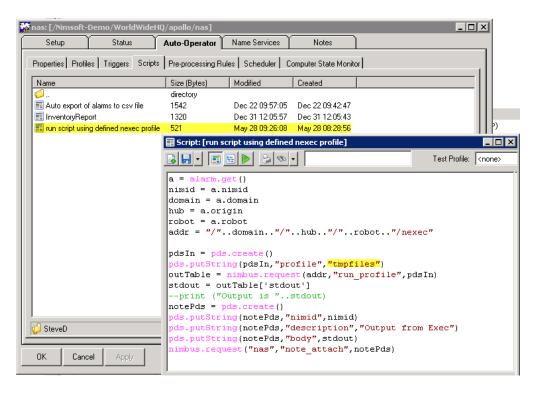
📽 Probe utility [/Nimsoft-Demo/WorldWideHQ/apo	llo/nexec]	_ 🗆 🗙
? 💽 💷 🕨 🔊		
Probe commandset	Command output (run_profile)	
run_profile	Na Value stdout Volume in drive C has no label II Volume Serial Number is 400F-98FE IIII Directory of C:\WINDDWS\TE	4Pmm05/29/2010 12
Parameters	stderr	M 11105/20/2010 12
Name Value	return 0 profile tmpfiles	
profile tmpfiles	Promo emprinov	
profile		
Impfiles	۲	Þ
	,	
Command status : OK		192.168.128.10

Useful feature: You can add the stdout/stderr to a note contained in an alarm.

Automatic execution of actions, e.g., using commands/scripting

Nas probe (Nimsoft Alarm Server)

You have many options available to you to control <u>when</u> you run a LUA script to execute the command(s) by using the features of nas, e.g., based on operating period, schedule, excluding maintenance periods etc. First you create/add the script to your nas probe under scripts then under the Auto-Operator profiles...



and then you can choose when you want to run the specific script that executes the custom action/command, e.g., when you receive a message with the message text of "something failed" and it's a **critical** alarm.

		Computer State Monitor
Profile: [nexec demo		
Action type script	Action ca	tenoru 🔽 🧖
		Action mode
Carliet		On message arrival
Script I run script using define	ad navac profile	C On overdue age 5m 🝸
Script Parameter		C On every AO interval
		C On every interval 5m
12N		C On trigger
Severity Level		Message Visibility ignore 💌 🔄 NimBUS Domain
Hostname Subsystem ID.	Source hostname1 Subsystem String	NimBUS Domain
Hostname	Source	NimBUS Domain
Hostname Subsystem ID. User Tag 1	Source hostname1 Subsystem String User Tag 2	NimBUS Domain
Hostname Subsystem ID. User Tag 1 Message assigned	Source hostname1 Subsystem String User Tag 2	NimBUS Domain
Hostname Subsystem ID. User Tag 1 Message assigned <any></any>	Source hostname1 Subsystem String User Tag 2	NimBUS Domain NimBUS Hub Name NimBUS Robot Name NimBUS Robot Name NimBUS Probe Name
Hostname Subsystem ID. User Tag 1 Message assigned	Source hostname1 Subsystem String User Tag 2	NimBUS Domain

To test your Auto-Operator profile to see if it is successfully executing the action, you can go to the Status Tab in the nas and Send a Test Alarm via rt-click.

🚰 nas: [/Nimsoft-Demo/WorldWideHQ/apollo/nas]							
Setup Status Auto-Operator Name Services Notes							
Alarm Status							
critical major minor warning information Total alarms	274						
Last alarm May 2	28 09:57:31						
41 118 62 39 14 Last event May 2	28 10:00:15						
Alarm Messages Alarm properties							
Time of origin H Message text	Severity 🔺						
May 19 14:05:31 nin something failed 9 3.1.9	major						
Alarm 5 Alarm	major						
May 26 10:59:16 ap 1.1 NimBUS Alarm 2 Oracle	major						
May 26 10:55:30 ex 1 NT-Service	s major						
May 26 10:56:25 as Severity level Source of sender 0 2.3.3.3	warning						
May 26 10:56:26 as critical v hostname1 0 2.3.3.3	warning						
May 26 10:59:28 19 Suppression key 5 Network	major						
May 26 10:59:28 10 5 Network	major						
May 26 10:59:29 ae 7 Network	minor						
May 26 10:59:29 ap	s major						
May 26 10:59:30 19 Send Cancel 5 Network	major						
May 26 10:35:07 citu	minor						
Average Ave	minor						
Average Ave	minor						
Available May 26 10:59:43 nim-rwc-rout RTR 4: The 'echo' probe configuration is not available. 565 Network	major						
Av 26 10:59:43 nim-rwc-rout RTR 1: The 'echo' probe configuration is not available. 565 Network	maior 🔳						
Version 3.31, Feb 8 2010. Started May 10 14:40:10 Total	274						
	214						
OK Cancel Apply	Help						

In the alarm sub-console in the Infrastructure Manager, you can use the alarm filtering feature to see if you got the test alarm:

Alarm Filter	×
Alarm Source	
Source: hostname1 Time Origin: Older than 🔽 0 🐑 Hour	s affic
Nas: Time Arrival: Older than 🔽 🚺 Hour	
Origin: Assignment	her
Subsystem: Assigned To:	
Subsystem ID: Assigned By:	
Domain: Time Assigned: Older than 🔽 0 🔆 Hour	s (ICMP/TCP)
Hub:	- N Probe
Robot: User Tag 1:	her
Probe: User Tag 2:	onse
Message Count Severity Level /."something failed."/ >= 1 * >= Clear	3
OK Apply Reset Cancel Help	Tot: 91, Sel: 1
⊈⊈× ✓ \$ ₽ ₩₽ ₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩	
I., Host Name Δ Source Message	
hostname1 hostname1 something failed	

You can then open the alarm and read the notes on the alarm and of course, operators can add their own comments to it.

Alarm Details			x	Notes
ID: HT46709776-71767 Source: hostname1 Domain: Nimsoft-Demo Nas: WorldWideHQ Subsystem: Alarm (1.1) Message: something failed	Host Name: hostname1 Probe: Robot: apollo Hub: WorldWideHQ Severity: Critical	A	Accept Assign Unassign Acknowledge History Notes	Output from Exec Volume in drive C has no label. Volume Serial Number is 400F-98FE Directory of C:\WINDOWS\TEMP 05/28/2010 12:34 AM <dir> 05/28/2010 12:34 AM <dir> 03/18/2010 04:33 PM <dir> 03/18/2010 04:33 PM <dir> 03/18/2010 04:33 PM <dir></dir></dir></dir></dir></dir>
Count: 2		<u>_</u>	Previous Next	axis2-tmp-1785578851293540036.tmp.lck 05/04/2010 06:40 AM <0IR> axis2-tmp-1918306354180492228.tmp 05/04/2010 06:40 AM 0 axis2-tmp-1918306354180492228.tmp.lck
Time Received: May 28 2010 09:54:50 Time Origin: May 28 2010 09:44:25 Time Arrival: May 28 2010 09:44:26 Origin: WorldWideHQ User Tag 1: MSSQL	User Tag 2: YourGroup		Help	04/23/2010 04:59 PM <dir> axis2-tmp-2286142142859608423.tmp 02/22/2010 12:37 AM <dir> axis2-tmp-2908769743207110987.tmp 02/22/2010 12:37 AM 0 axis2-tmp-2908769743207110987.tmp.lck</dir></dir>
erver				OK Comment

Summary

- nexec probe can be deployed to the various robots with profiles configured to run the desired scripts/commands. These profiles can be executed via LUA <u>script</u> from the nas (central point) via nimbus.request() calls in response to specific alarms.
- If you want to "trigger" actions locally rather than from the nas using a script you can also use probes if they support actions it depends on the probe. The only local 'agent' ones possible are through probes that provide that capability for example, logmon, dirscan, processes, can run commands and it does not require anything else.
- If these are a set of standard options then configuring them via nexec and then calling them via a callback from nas/LUA. It depends on what reporting you are looking for on the actions.
- If nexec probe is not an option, then possibly a custom on-demand probe will work that can run the required action.

We have created scripts/probes to run commands remotely (e.g. via ssh or pscript), but then authentication becomes the key – see rsp probe.

Reference: Nexec demo script with comments

-- Get the alarm object
a = alarm.get()
-- Extract the NimID from the alarm object
nimid = a.nimid
-- Extract the address details from the alarm object
domain = a.domain

hub = a.origin robot = a.robot -- Construct the address as /domain/hub/robot/probe addr = "/"..domain.."/"..hub.."/"..robot.."/nexec"

-- Create a PDS object to use to send details pdsIn = pds.create()-- Add a string key/value pair to the PDS to tell the probe which profile to run pds.putString(pdsIn,"profile","interface info") -- Run the "run profile" callback of the nexec probe outTable = nimbus.request(addr,"run_profile",pdsIn) -- Take the "stdout" parameter from the returned table stdout = outTable['stdout'] -- Create a new PDS to use to construct a note notePds = pds.create() -- Add key/value pairs to the PDS to define the NimID, Description and body pds.putString(notePds,"nimid",nimid) pds.putString(notePds,"description","Output from Exec") pds.putString(notePds,"body",stdout) -- Run the "note attach" callback of NAS to attach a note to the NimID nimbus.request("nas","note_attach",notePds)