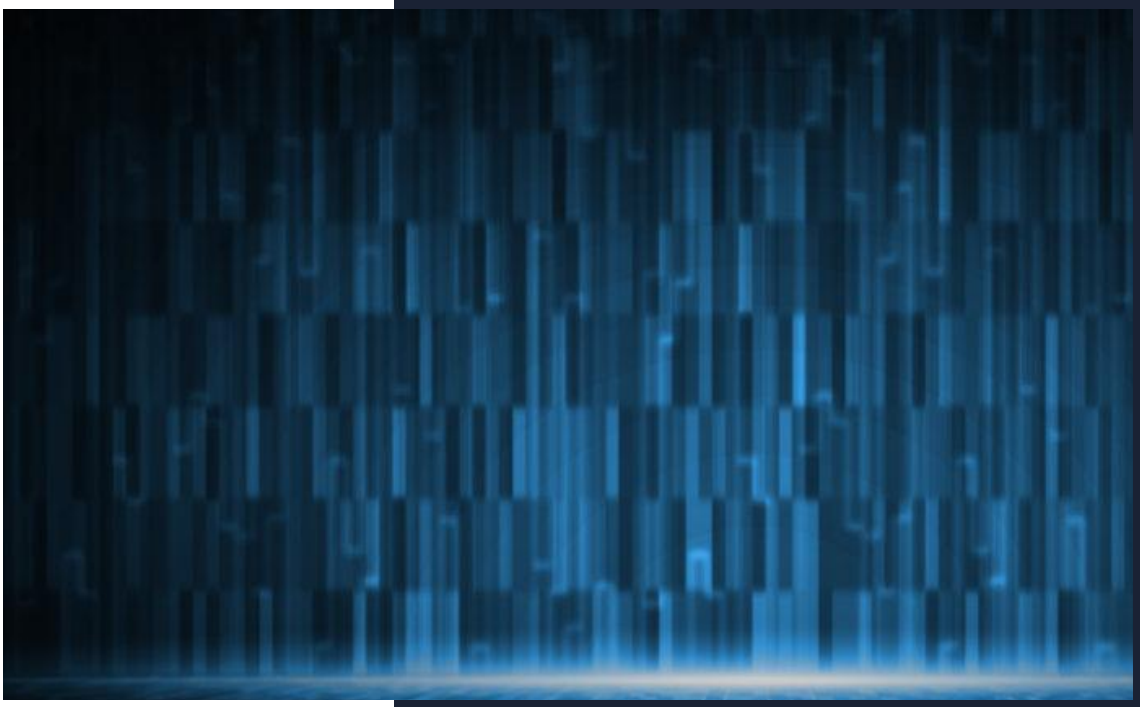
AMDO SOFT
ROBOTIC · PROCESS · AUTOMATION

ROBOTIC PROCESS
AUTOMATION
SYNTHETIC MONITORING
IT AUTOMATION
IT MONITORING



IT Automation Rule Templates

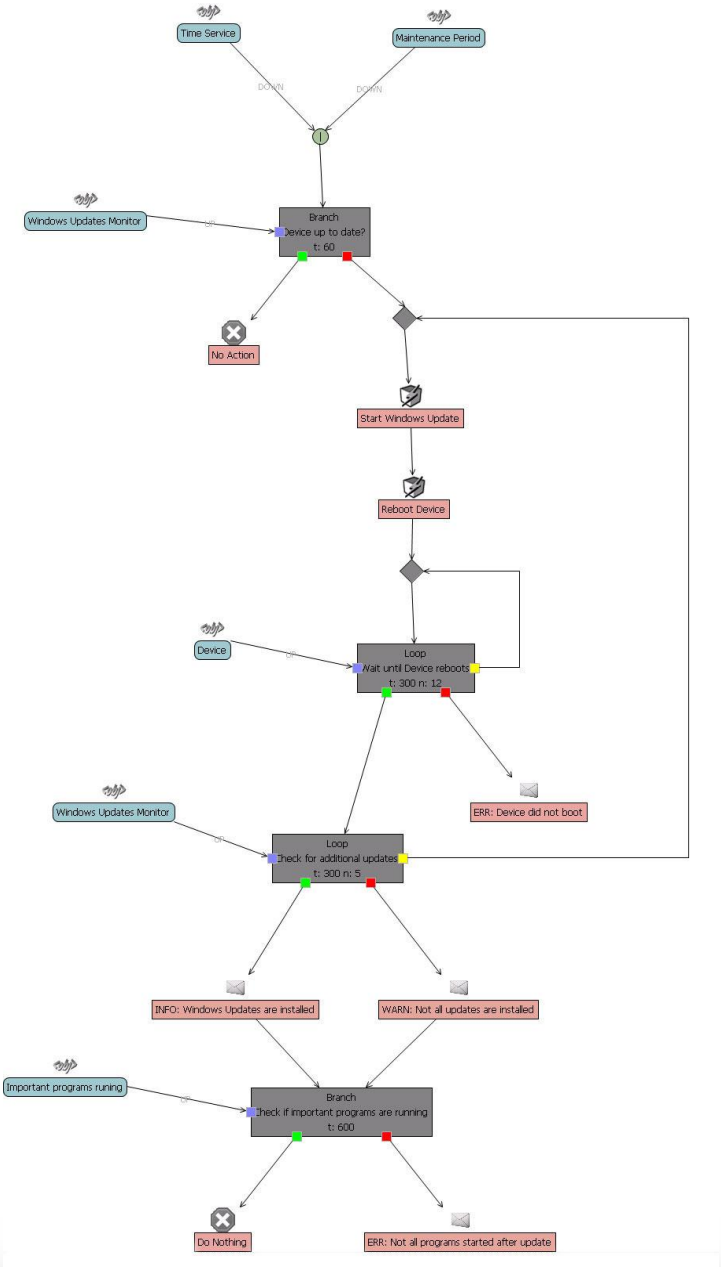
Table of Contents

Automating Windows Update

TASK: Start Windows Update at specific time point in month and install new updates. Afterwards we restart machine and check if new updates are available and repeat process. At the end we have to check if all important services are running (e.g. Exchange Server, Outlook Web Access, etc.)

SOLUTION: Once triggered by Time Service (e.g. at specified date/time in month or during the ad-hoc defined maintenance period), b4 is going to start installing Windows Updates, restart operating system and afterwards check if another updates are required. At the end of update it checks if important programs are running.

RULE:



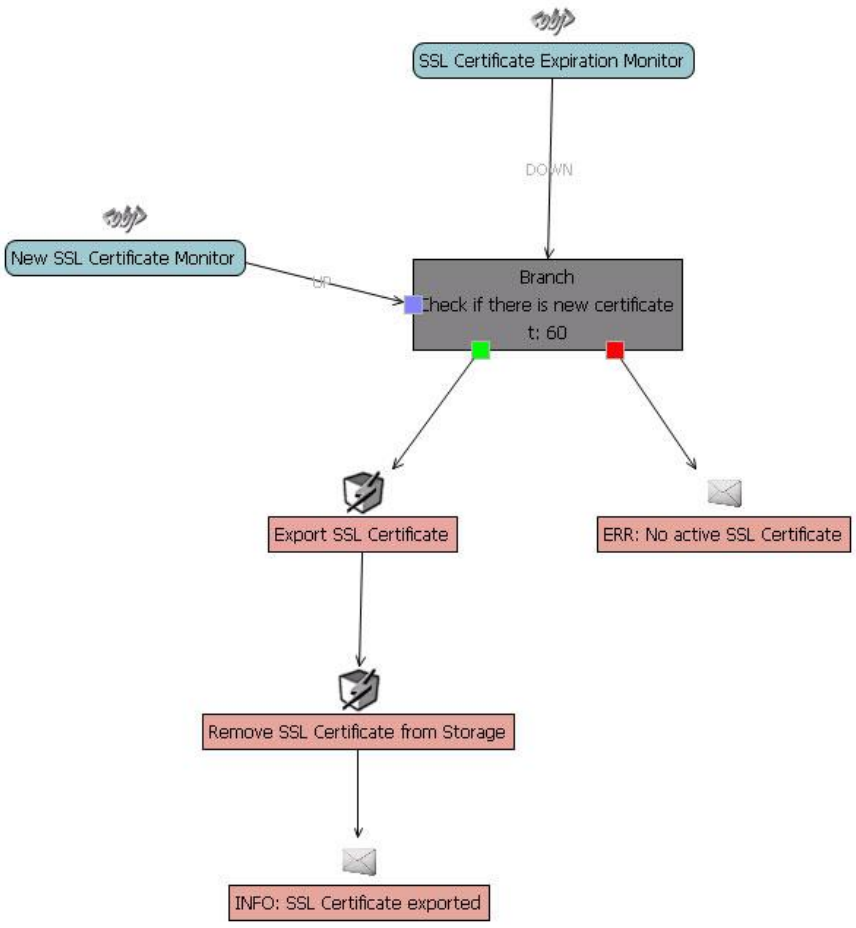
Automatic SSL certificate management

TASK: Check if SSL-Certificate has expired. Then we need to check if there is new certificate ready for that particular Domain. If there is new certificate we need to backup the old one (export) and remove it from Certificate Storage.

SOLUTION: We can use various utilities and scripts in order to check and manipulate certificates. In order to have this automation we first need the monitor that checks if certificate has expired. This can be done by making custom monitor (script). Such monitor will go to DOWN state when certificate expires. Then we can create rule which will trigger once monitor goes DOWN. Also, we will require second monitor that checks if there is new certificate for specific domain (custom monitor).

Once rule triggers it first checks if there is new certificate for specified domain. Then if there is no new certificate the rule will send e-mail informing you about it. In case there is new certificate script is called which exports the old certificate and removes it from certificate storage. At the end the rule informs us what has been done.

RULE:

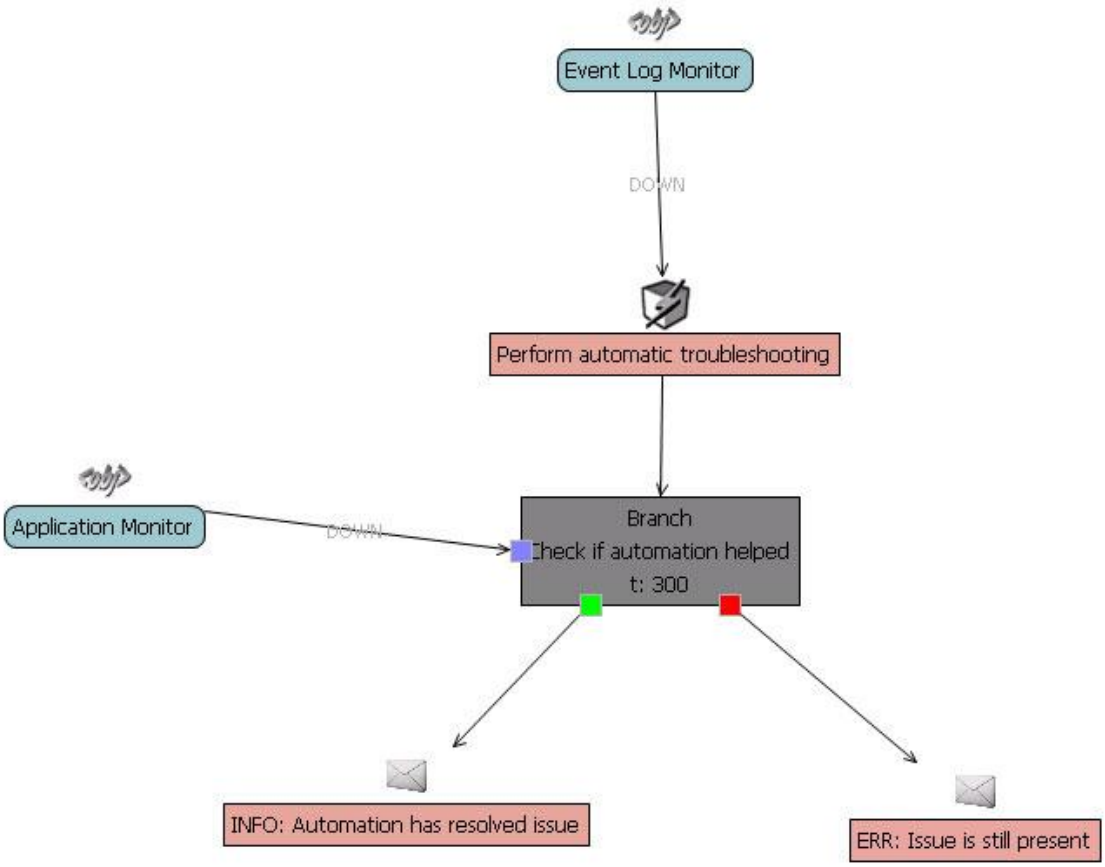


Automatic resolving of specific issues reported in event log

TASK: Error event ID 1, with SQLVDI as source, appears in massive numbers. We need to investigate and resolve such errors. Error description usually contains TriggerAbort, SVDS::CloseDevice or SignalAbort. Rest of the message is usually the same.

SOLUTION: If we know how to resolve the issue, reported in particular event ID, we can automate it. In that case we can create Event Log monitor which would check if event ID 1 with specific keyword appeared (e.g. TriggerAbort), This monitor is used to trigger rule which then calls automation script. After the script is over we can check to see if everything is fine (e.g. service monitor to check if service is running).

RULE:

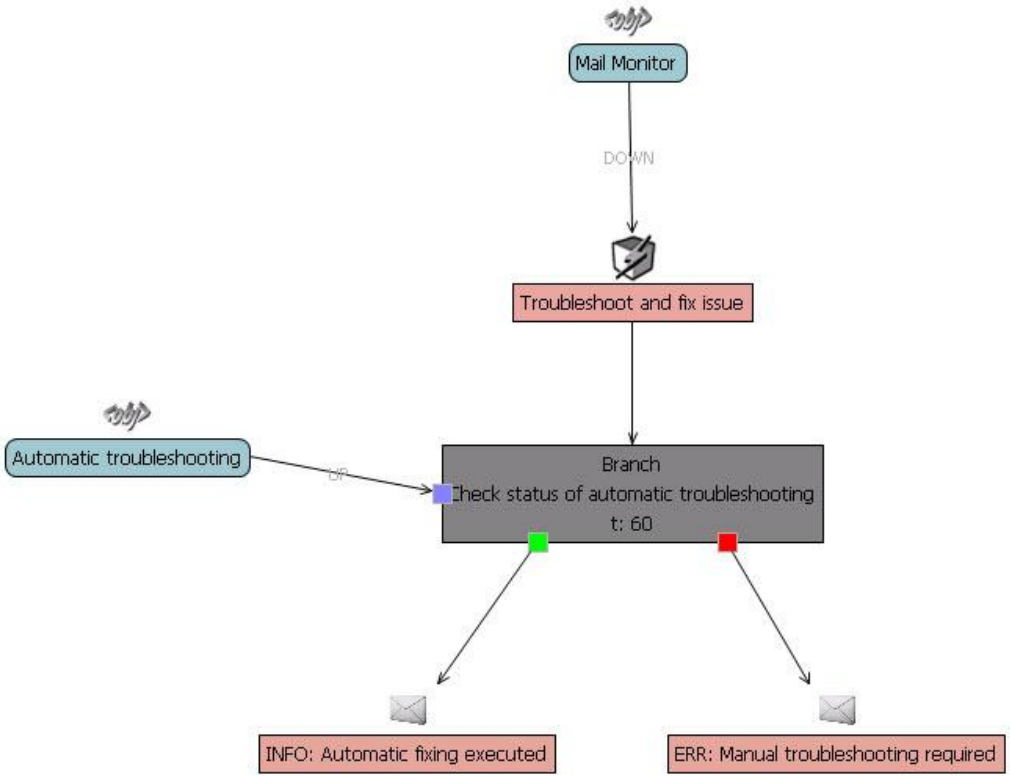


Automatic resolving of Exchange e-mail availability issues

TASK: E-mail from Exchange is returned with error message to user. We need to analyze error, conclude what is causing issues and resolve it.

SOLUTION: We can monitor Exchange logs to see if e-mails have bounced. When an error appears we can then use that monitor to trigger automation which will fix known issues using scripts. Script which we use for fixing issues will be executed from Execute Command Service so after script runs through it we can see if it was known issue or not. According to the execution result we can at end send an e-mail informing what rule has done.

RULE:

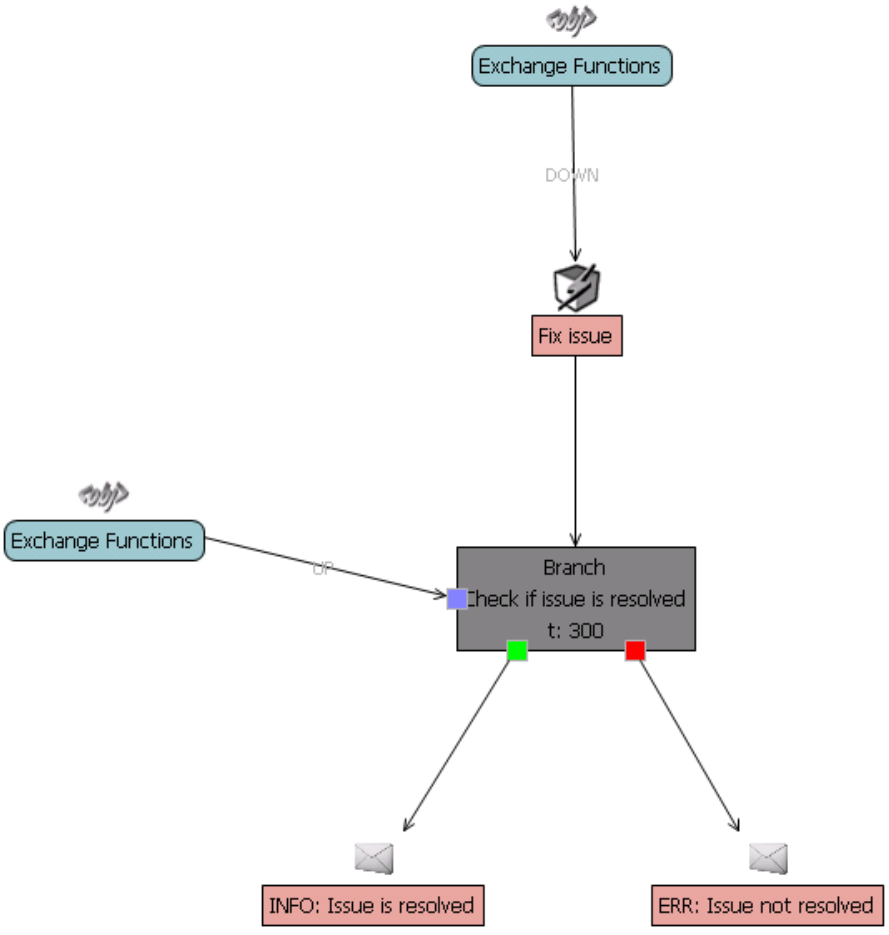


Prevention of Exchange issues

TASK: User reports connection issues between his iPhone and Exchange. We need to check server and resolve eventual issues.

SOLUTION: We have different approach to this. We check Exchange all the time and if something happens we use the rules to resolve various issues. This means that, ideally, issue is resolved before user even notice it.

RULE:



Automatic resolving of OWA issues

TASK: Outlook Web Access is no longer accessible. Event log describes an error in IIS configuration file. We need to restore that configuration file using ShadowProtect and restart IIS. If error repeats we need to restore older version of file.

SOLUTION: In order to have such automation we need two monitors:

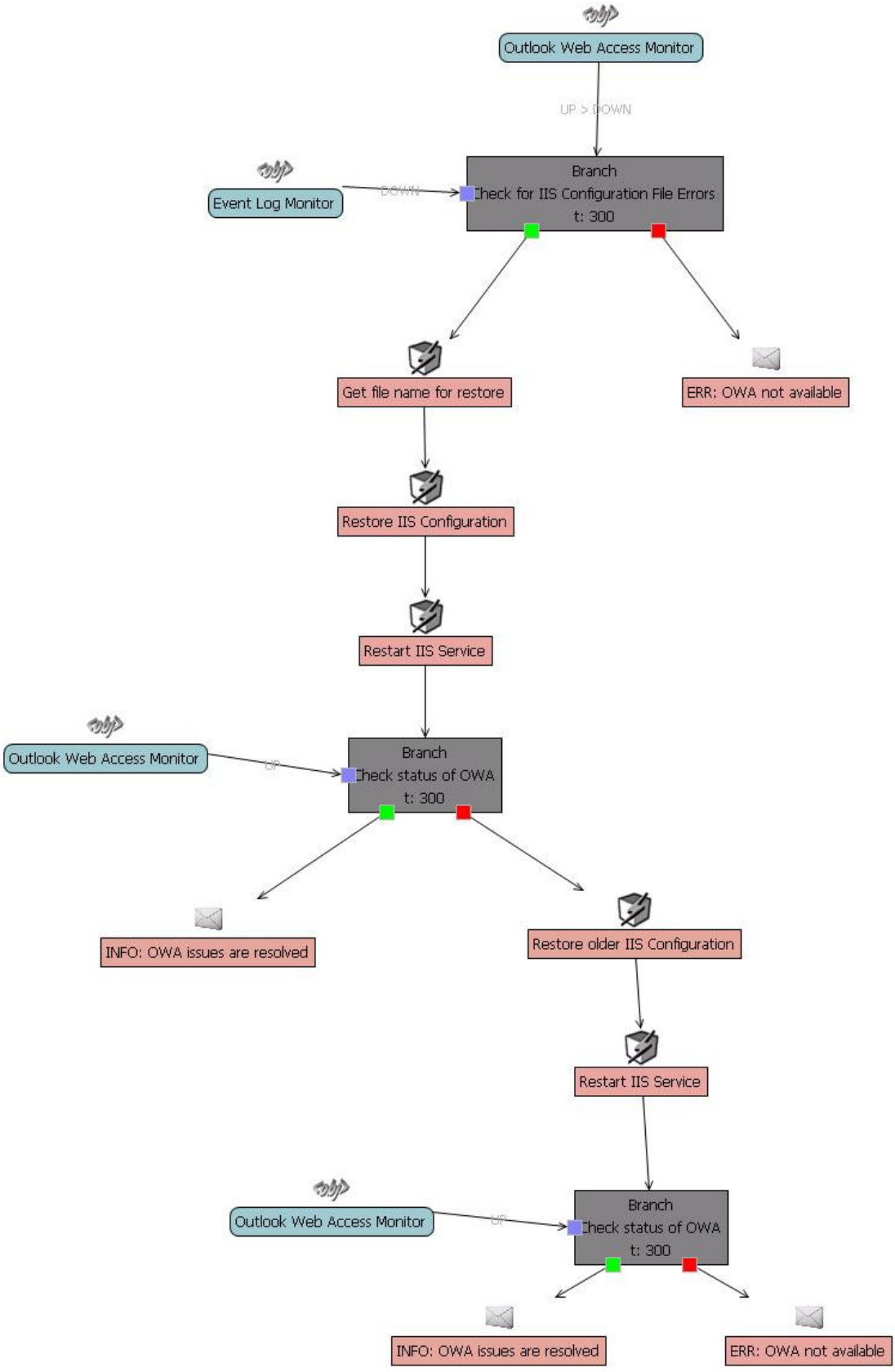
- URL monitor which will check availability of Outlook Web Access
- Event Log Monitor which will check for particular IIS issues

We will use these two monitors in rule. First one will be trigger and second one will be used to check if we have issue with IIS configuration or maybe something else is causing OWA issues (e.g. internet line break)

Now, if both conditions are met the rule will execute script (Execute Command Service) which will get path and name of file and then restore it from ShadowProtect backup. Next step in rule is to restart IIS (simply call small batch script that restarts IIS). And check if OWA is now working properly.

In case there are still OWA issues we call second script which, this time, restores older version of configuration file. We restart IIS again and check OWA. Depending on the result we send an e-mail that all is fine or that we still have some issues.

RULE:

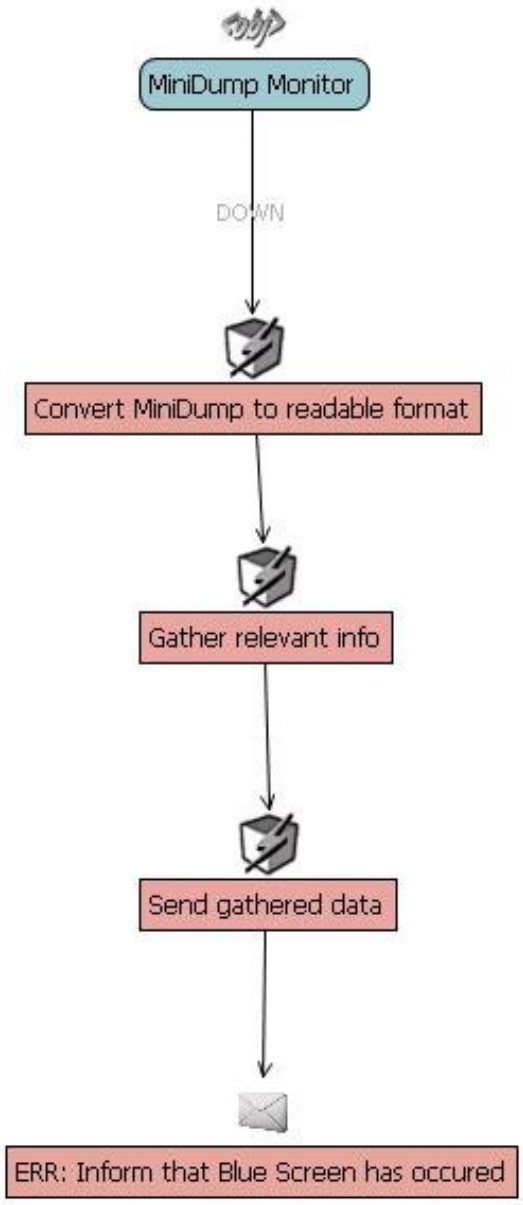


Reading core dumps and sending e-mail with important data

TASK: Machine has crashed with Blue Screen. We need to get MiniDump output in order to find out when file has caused it. Then we need to get informed about it including path and meta data of file (Manufacturer, version, etc.)

SOLUTION: In order to automate this we need monitor that checks if MiniDump file is generated (Blue Screen issue appeared). We will use that monitor as rule trigger. Once Rule is triggered we call scripts that converts MiniDump file to readable format and find entries that point to cause of issue. Then we call second script which will send that data to specified person (e.g. copy to share or send an e-mail with attachment).

RULE:

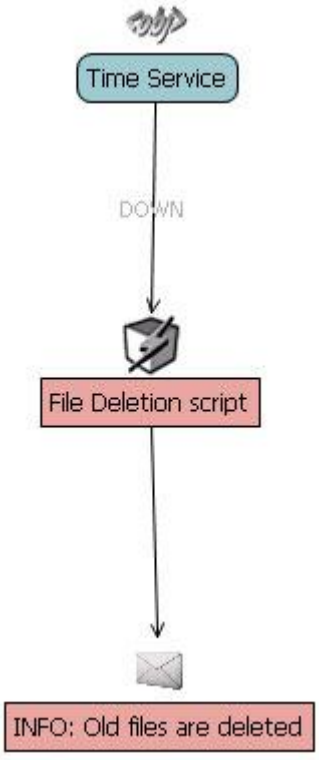


Scheduled deletion of old log files

TASK: Delete old, known, folders and log files (Exchange, IIS,…) regularly (e.g. older than 2 weeks).

SOLUTION: We can simply call script that deletes all files older then X day from specified folder(s) using Time service as rule trigger. Time service can be set to trigger at specific days/time.

RULE:



Automatic start of program if it is not running

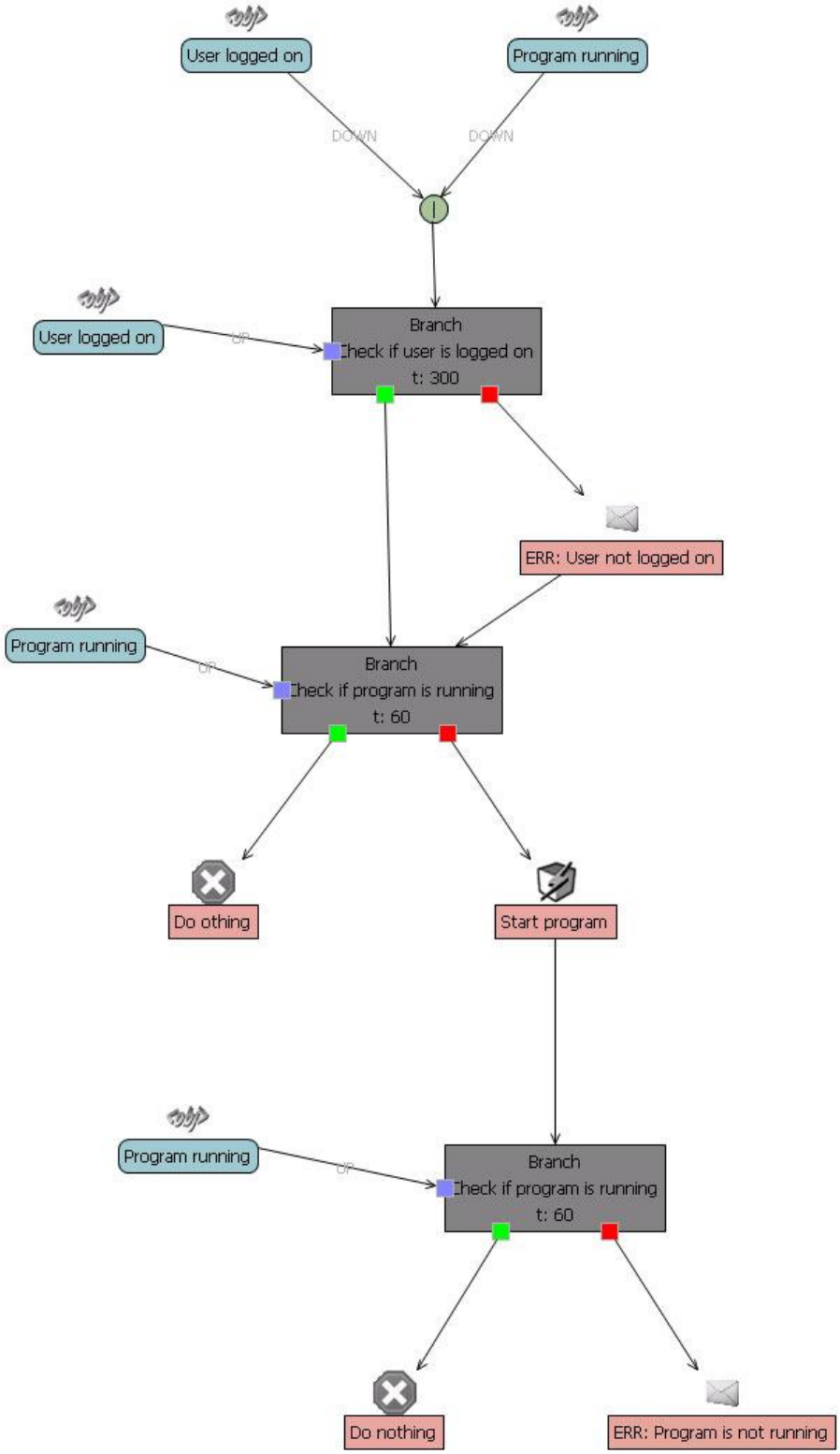
TASK: We introduced a new server for online banking software. For automated bank transfer there needs to be a user logged in even after restart.

Is it possible for the AmdoSoft agent to track, whether there is a user called svcMulti logged in, and if there is a Process called “loader.exe” running?

If it’s not running, would it be possible to send an e-mail? Or is it possible to log the user on and start the program via agent?

SOLUTION: It is possible to automatically log in to the machine after reboot. This is done by changing registry. Now we can perform b4 automation. For this we will use two Rule triggers: “User logged on” and “Program running” service. We set rule so either of those two can trigger rule. Once rule is triggered we check if user is logged on. If it is not then we send an e-mail. Regardless if user logged on or not we proceed with checking if program is running. If it is not running we call command or script to start it. Afterwards we check again if program is started. In case it did not start we send an e-mail that program starting was not successful.

RULE:

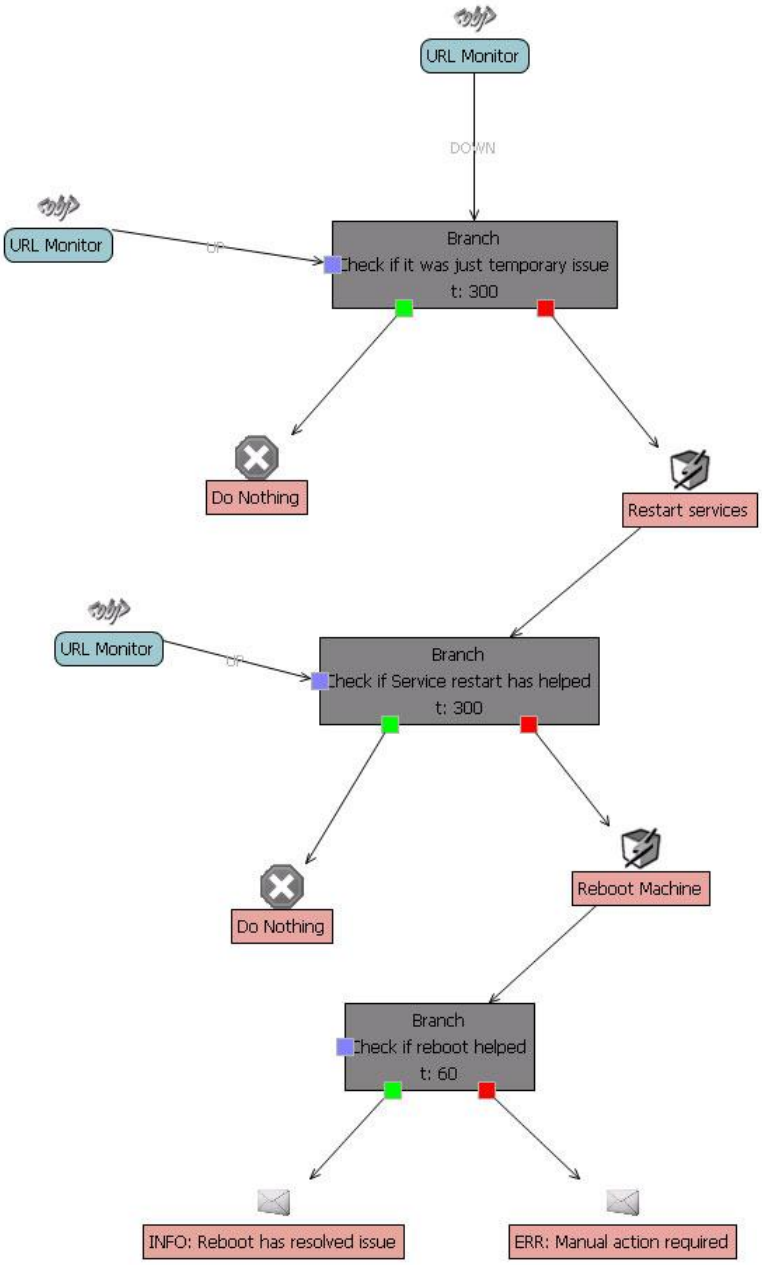


Automatic resolving URL availability issues

TASK: We need to monitor URL (web page) availability and when not responding immediately (or after certain delay) run stop and start commands on responding windows service, check URL availability once again, if still not available complete OS may be restarted.

SOLUTION: First we will need URL Monitor. We will use it as Rule trigger. Once rule starts we can wait for some time before proceeding with service restarting. Afterwards we check if service restart has helped, if not we reboot machine.

RULE:

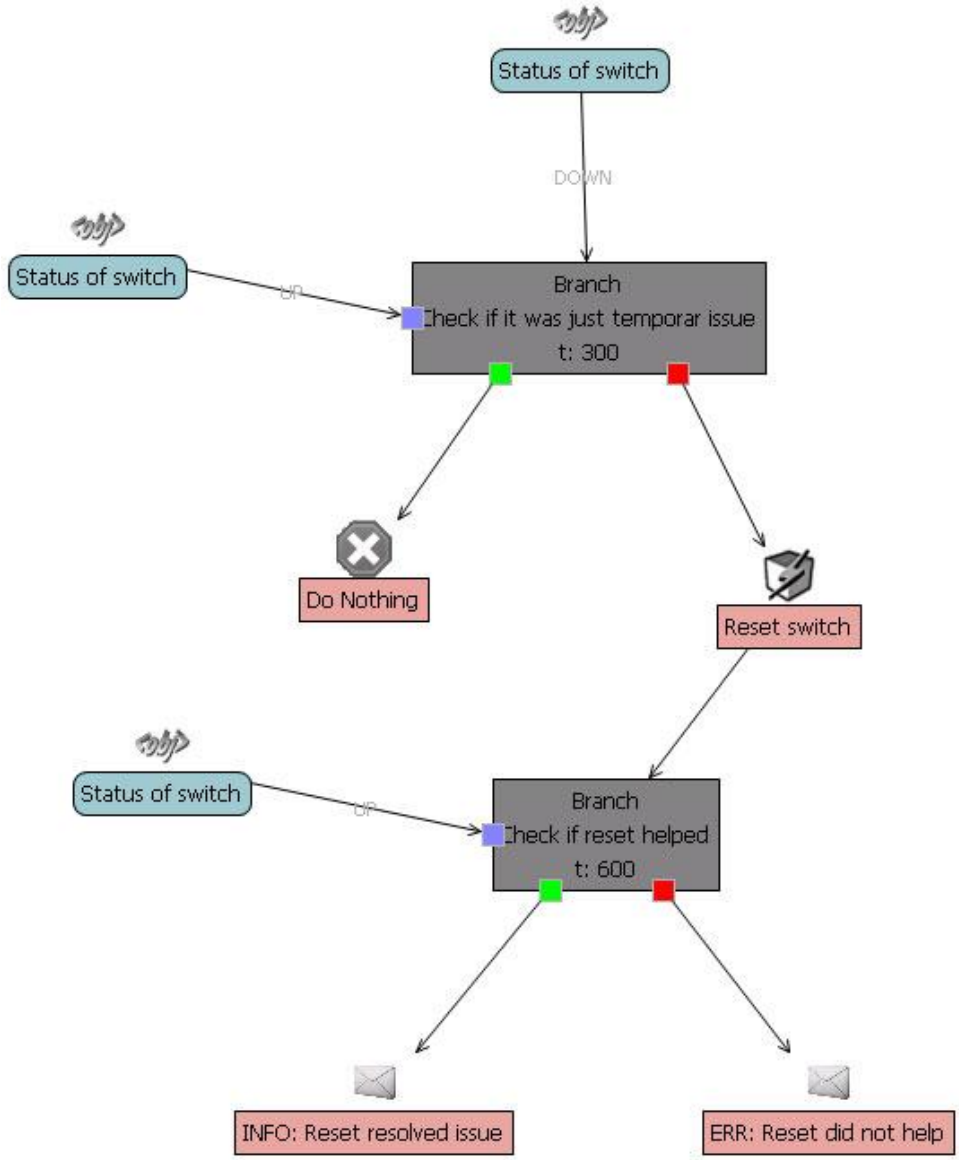


Automatic restart of Switch in case of issues

TASK: In case switch has issues we need to automatically restart it.

SOLUTION: For this we will need SNMP Management service which checks if there are any issues with switch. In case there are issues we then invoke SNMP-Set command from SNMP Management service which then resets device. Afterwards we check if reset has helped.

RULE:

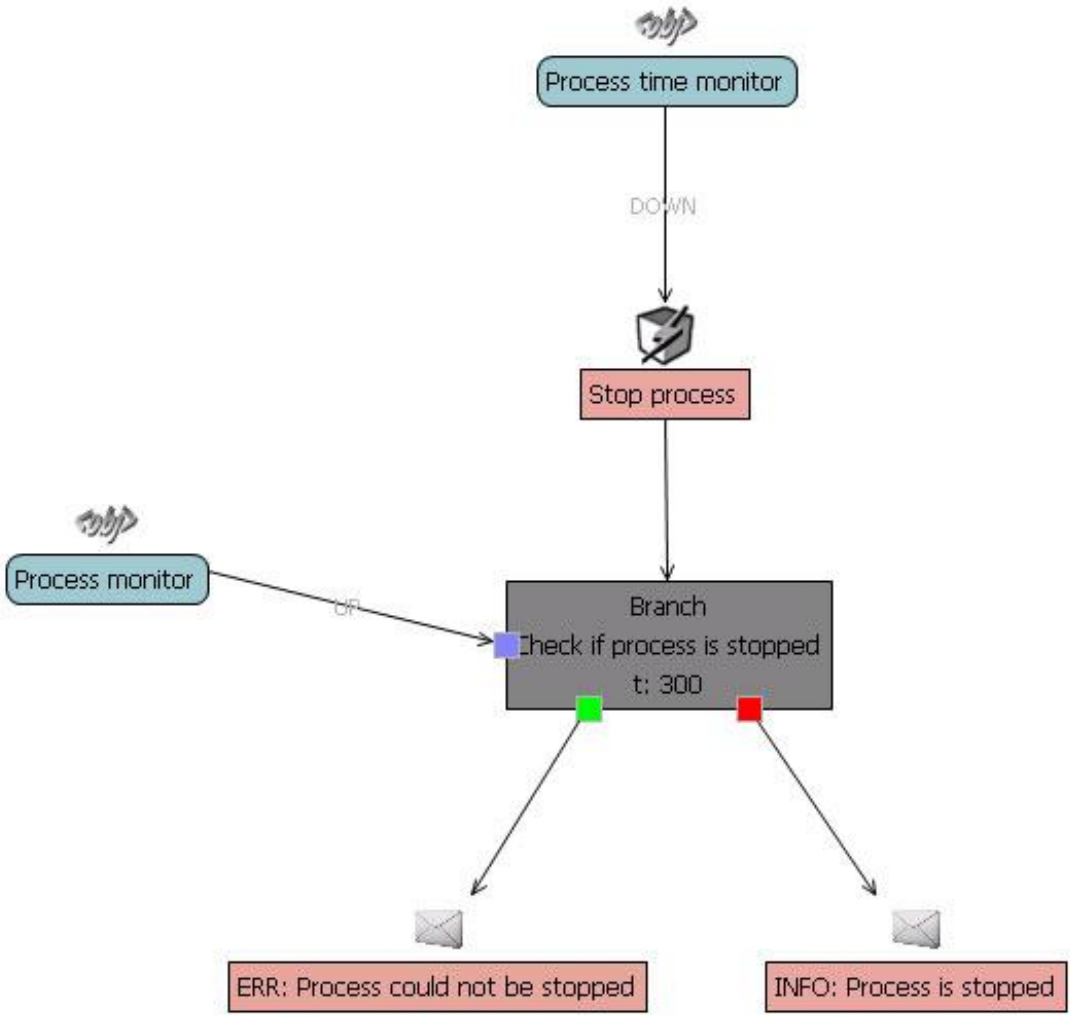


Automatic stopping of process if it is running for too long

TASK: We need to stop certain process if it is running for too long (e.g. Backup).

SOLUTION: For this first we need the monitor that checks how long is process running. Then we set thresholds so if process is running for too long monitor will go DOWN. When monitor is DOWN we simply call command that stops process. At the end we check if process is really stopped and send an e-mail.

RULE:

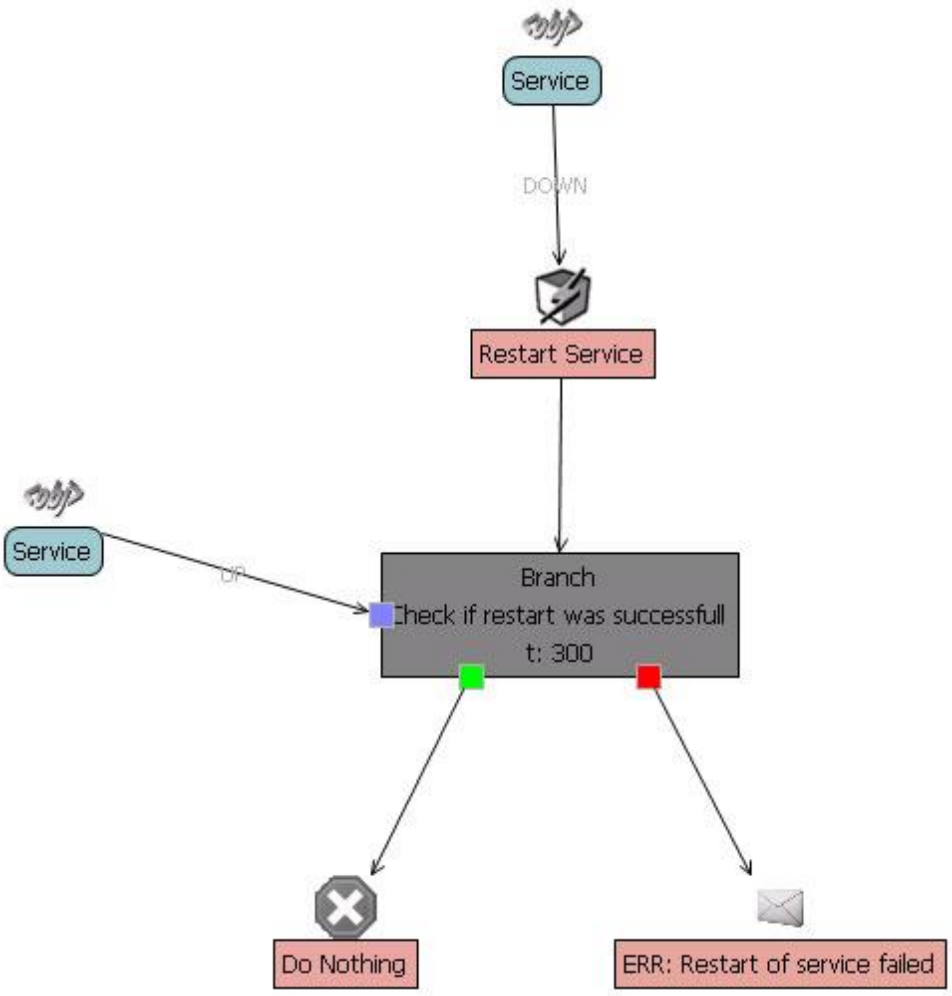


Start Service if it is not running

TASK: We have important services that we need to be running all the time. In case service is stopped we need it to be started automatically. In case of errors we need to be informed.

SOLUTION: For this we first need service monitor. We will use it as rule trigger. Once monitor goes down, service stopped, rule is triggered. Then we automatically call command to start it again. Then we check if start was successful. In case it could not be started we send an e-mail informing about it.

RULE:

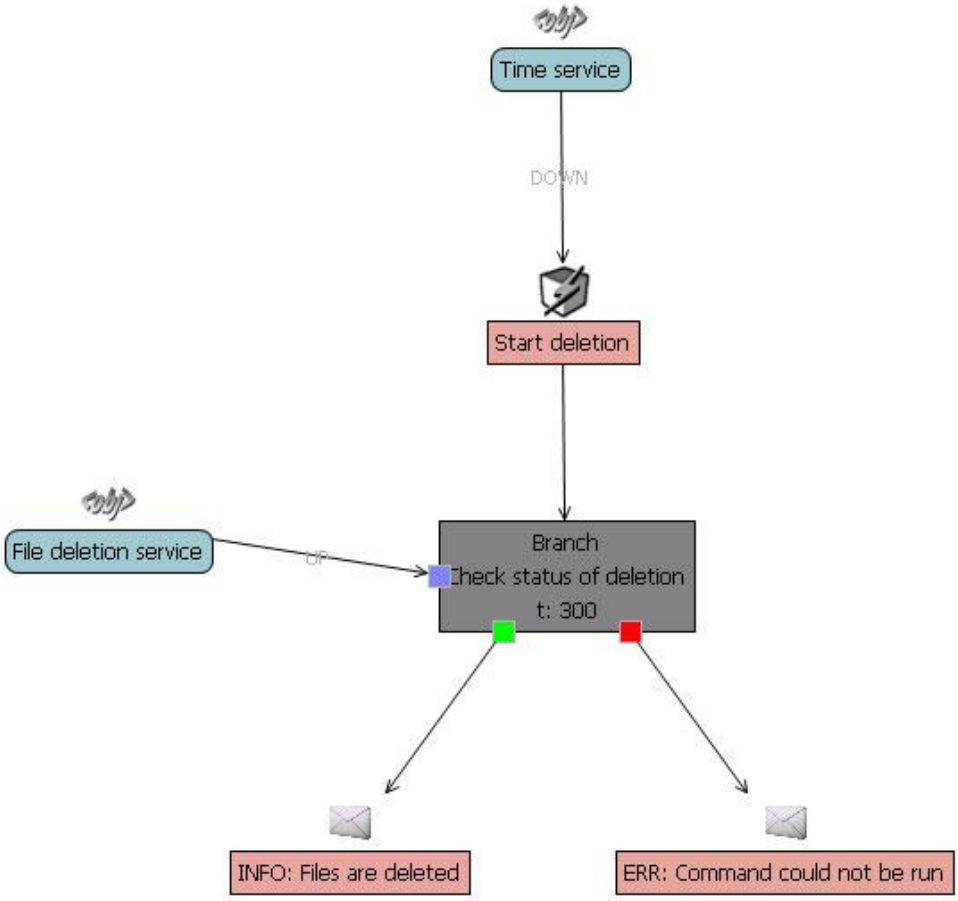


Automatic deletion of remote files

TASK: We have files on remote location (share) where we need to delete certain files. We can not install b4 Agent software there.

SOLUTION: We can mount share to existing b4 Agent and from there check which files are there. We can also create script that will delete files depending on parameters we use. This can be done automatically trough the rule. As a trigger we can use time service which would trigger the rule or set schedule (daily, weekly, etc). At the end we check if file deletion command has run correctly.

RULE:

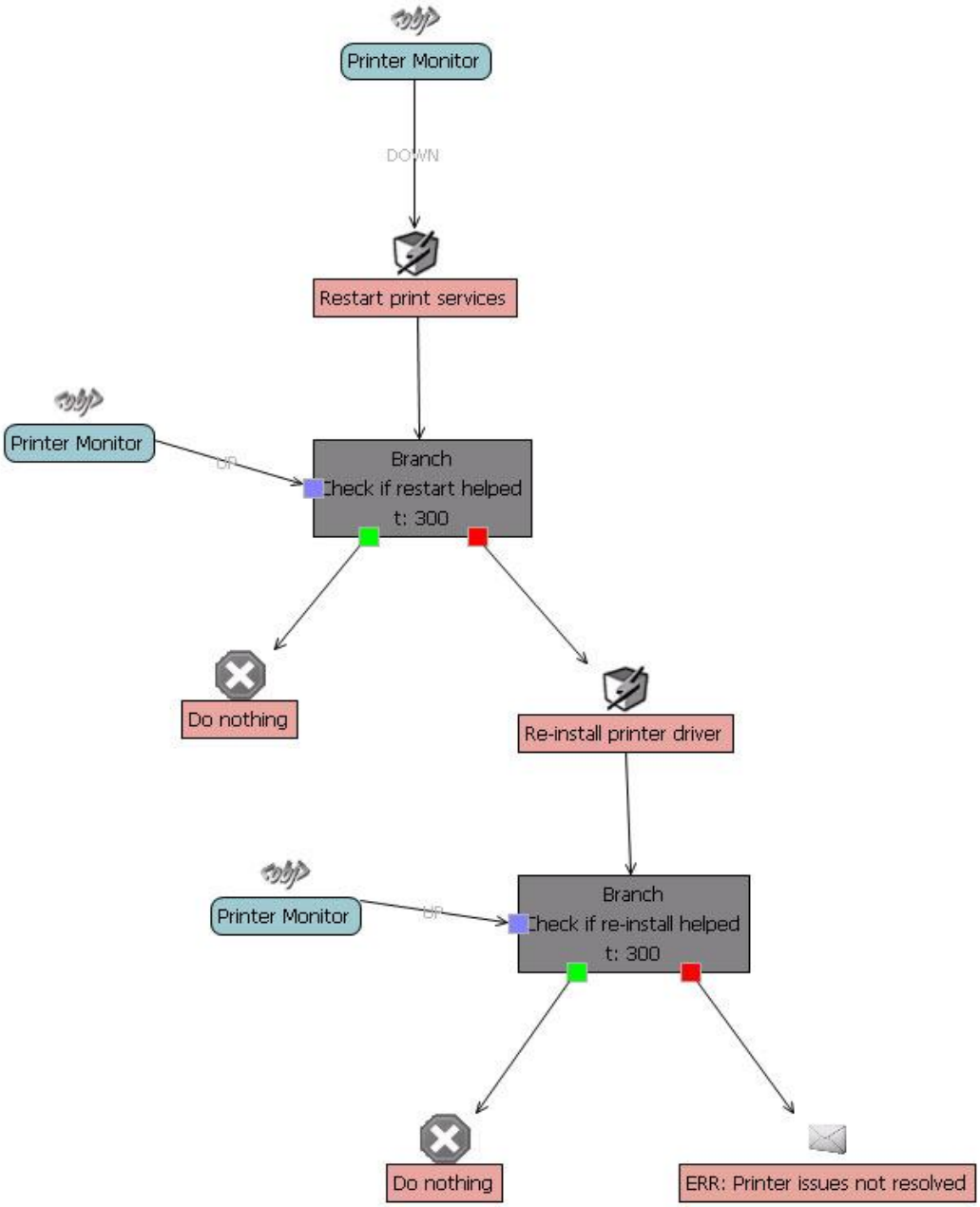


Automatic resolving of printer issues

TASK: We have many printers in our environment. Sometimes we have issues with printers. When such issue appears we need to restart print services and, if it does not help, we need to re-install printer driver.

SOLUTION: We can monitor printers to see if they are functioning correctly. We use same monitor as a trigger for rule. Once the monitor goes down we first restart services. If monitor is still DOWN then we call script that re-install drivers. At end we check if re-installation helped and, if not, send e-mail about issue.

RULE:

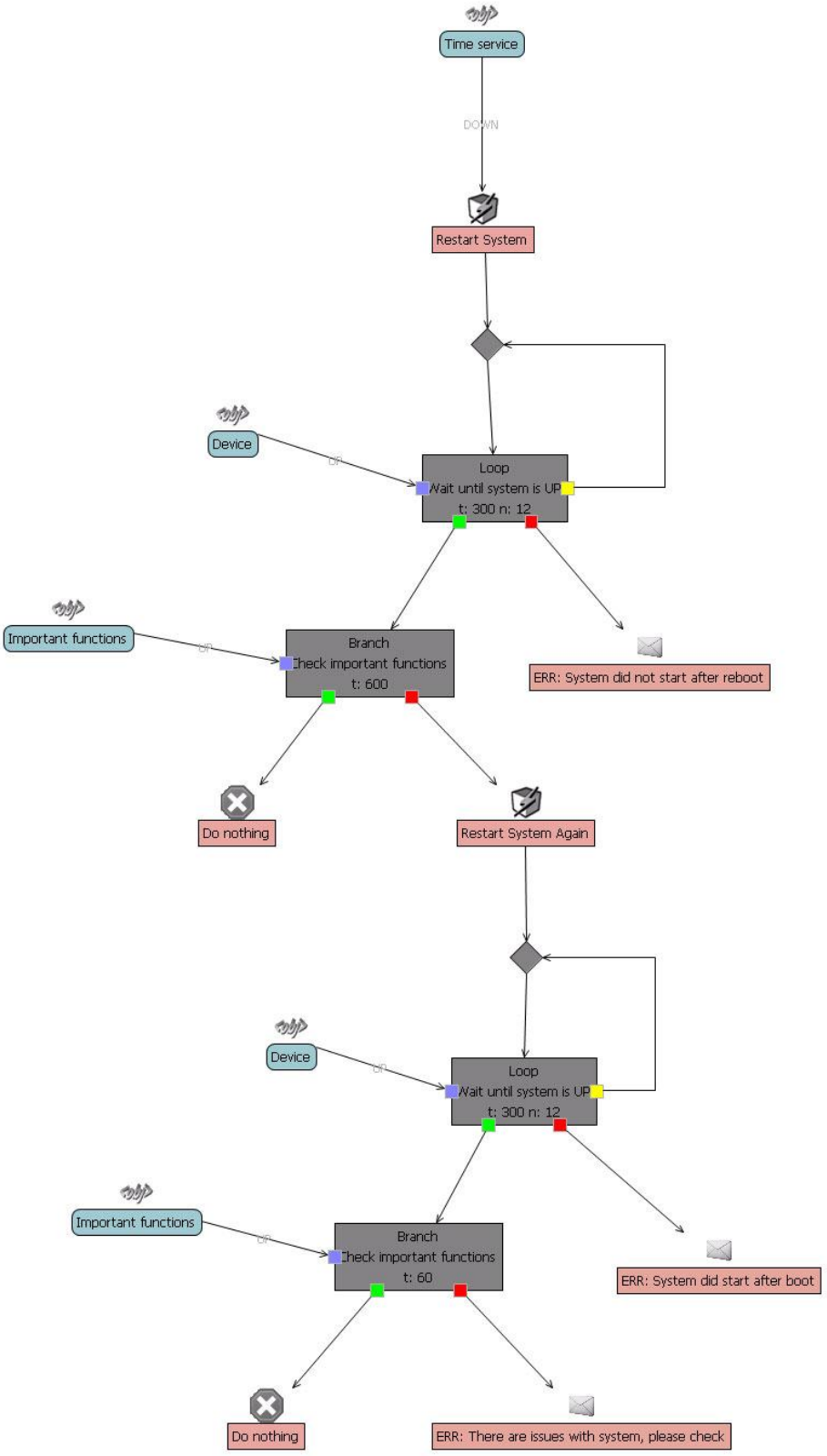


Periodical restart of operating system

TASK: We need to periodically restart of system on some machines. After restart we need to check if system is functioning correctly. If there are some issues we then need to restart it again.

SOLUTION: We can use time service in order to schedule system restarts. In order to check if all important functions are working we need to create monitors for them and then place all of them in a Service group. We will use status of the service group in order to check if all functions are working fine.

RULE:

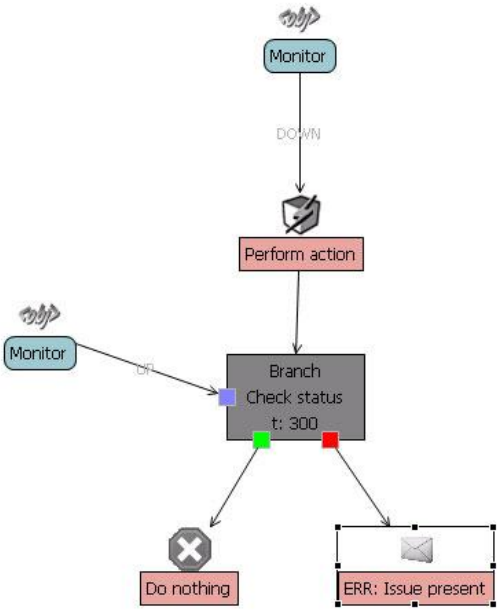


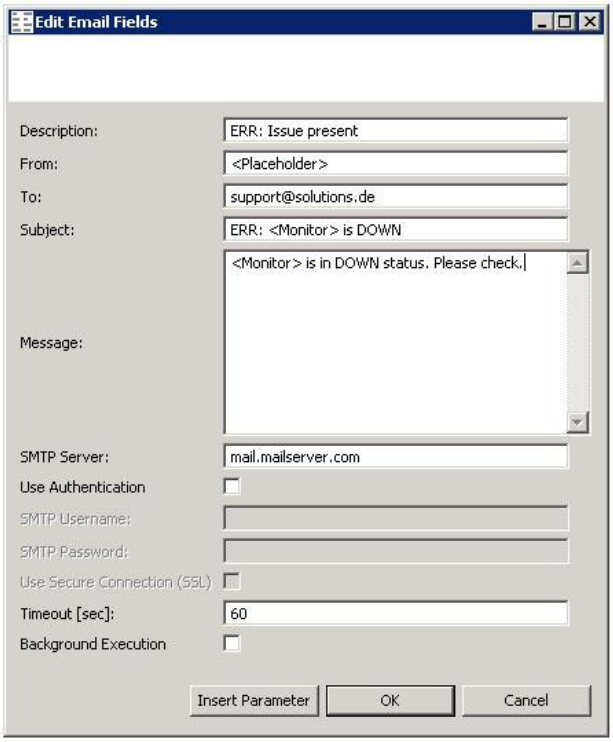
Add events to ticket management database

TASK: We are using TANSS ticket database for managing our support tickets. This software is able to recognize from e-mail address and use it to detect which customer has sent it. We need b4, when sending e-mails, to tell us at which customer issue appeared.

SOLUTION: We are able to set from field in e-mails we send from b4. Now when we create mailing action in rule template we use placeholder. When we create rules from templates then we can for each rule specify from field. This way we need one template for all locations instead creating separate templates for each one. This makes things much easier.

RULE:



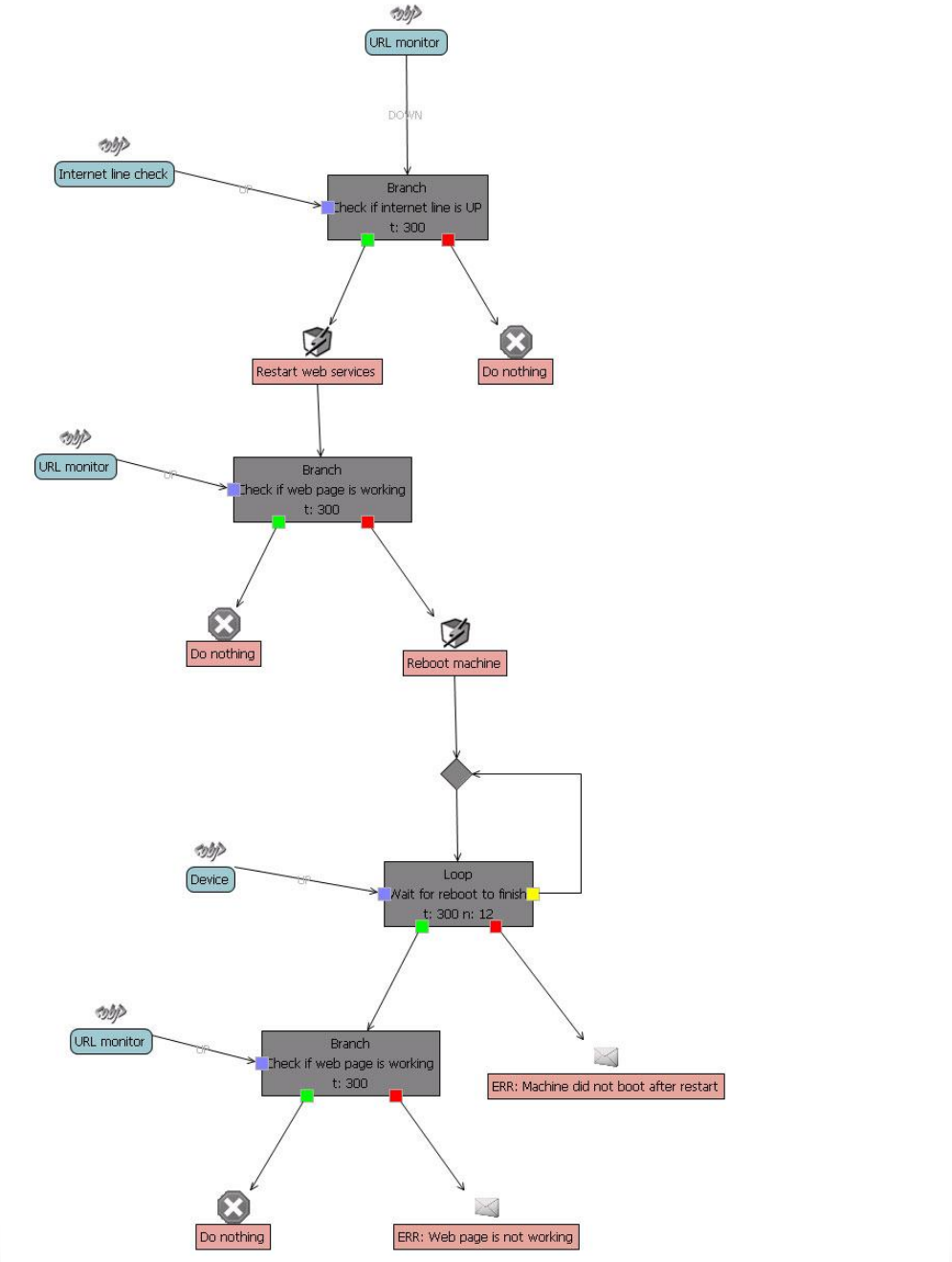


Web site recovery automation

TASK: We have important web server which needs to be working fine all the time. So what we need is to check if web page is available. If it is not we need to restart related services. If it does not help then we need to reboot machine.

SOLUTION: For this we can use URL monitor as trigger. URL monitor basically checks if specified web page is available. If it is not we need first to check if maybe internet line is down before proceeding further. If it is up next we restart related services. If that does not help either then we reboot machine.

RULE:

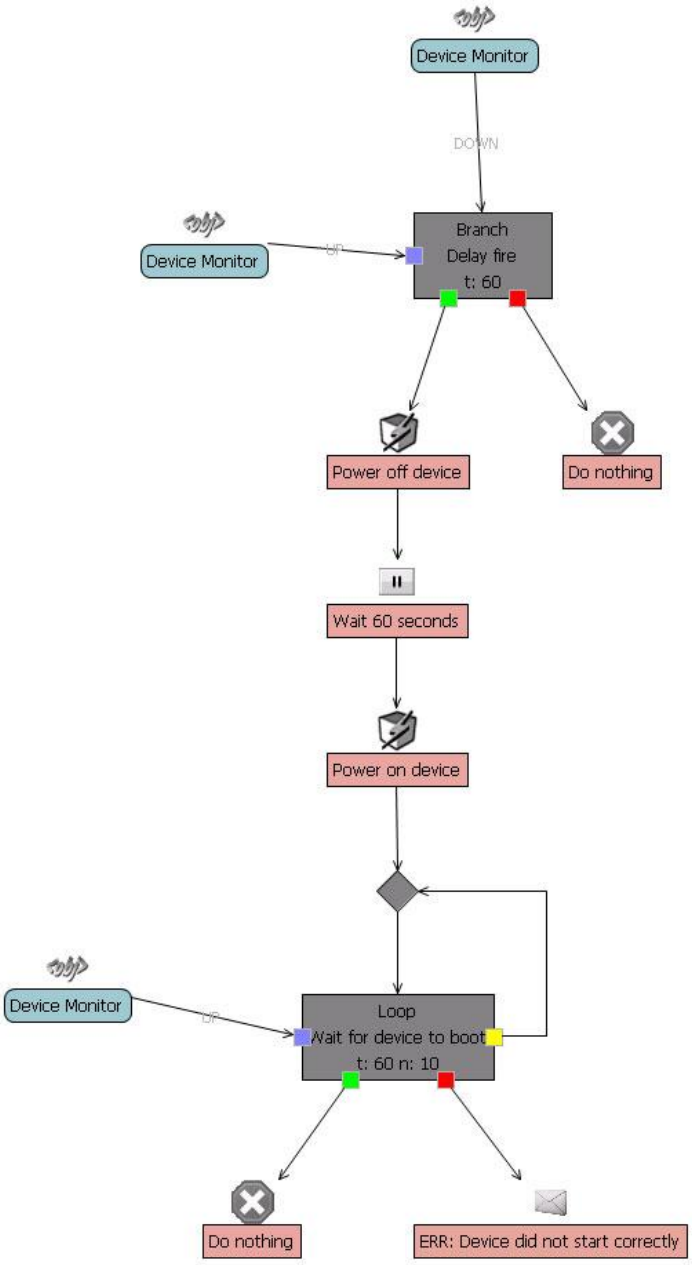


Network connectivity recovery

TASK: We have many devices in our network (Switch, firewall, etc). In case one of devices is malfunctioning we need to reset it in order to restore network connections. All devices are connected to APC.

SOLUTION: We are able to monitor ig network segments are reachable. In case some device is not reachable we can restart it over APC (power off/power on).

RULE:

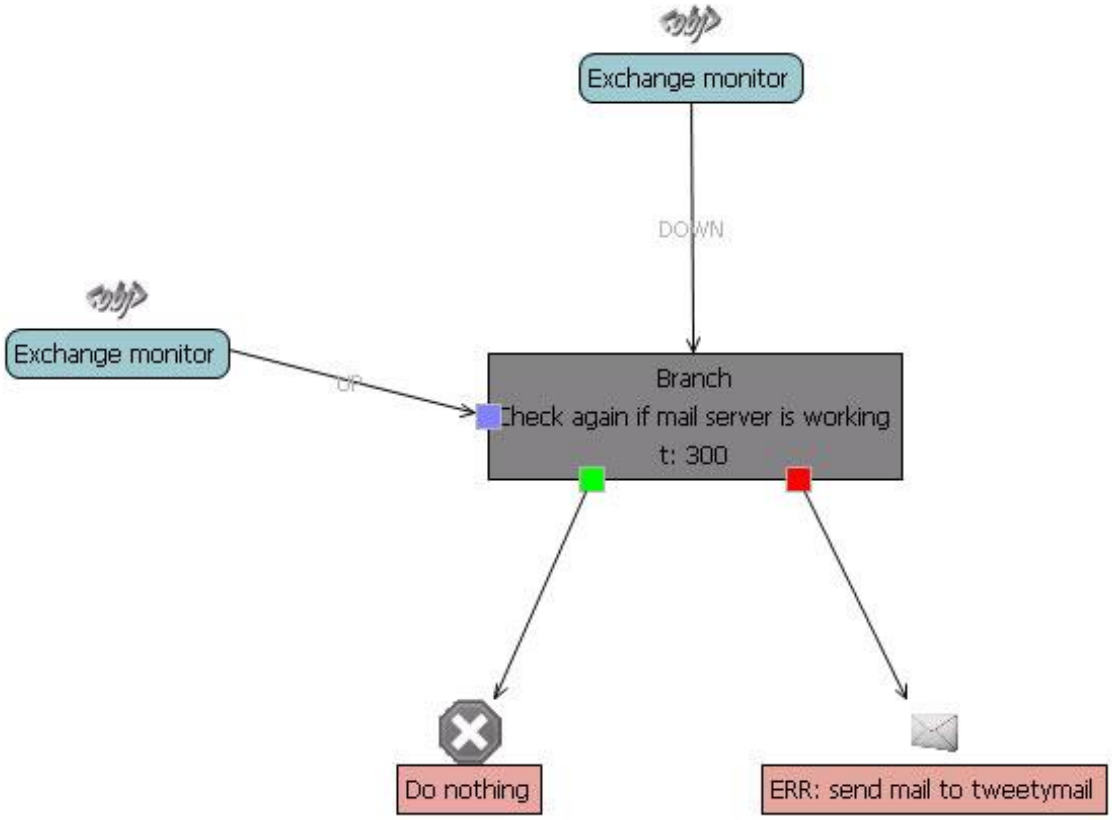


Alert when mail server is down

TASK: We need to be informed when mail server is down. Ideally it would be great if we can get tweet over tweeter when such thing happens so we can react to it.

SOLUTION: We have the monitor that checks if e-mail is working. In case it does not work we are able to send an e-mail to tweetymail service using different mail server which then sends tweet.

RULE:

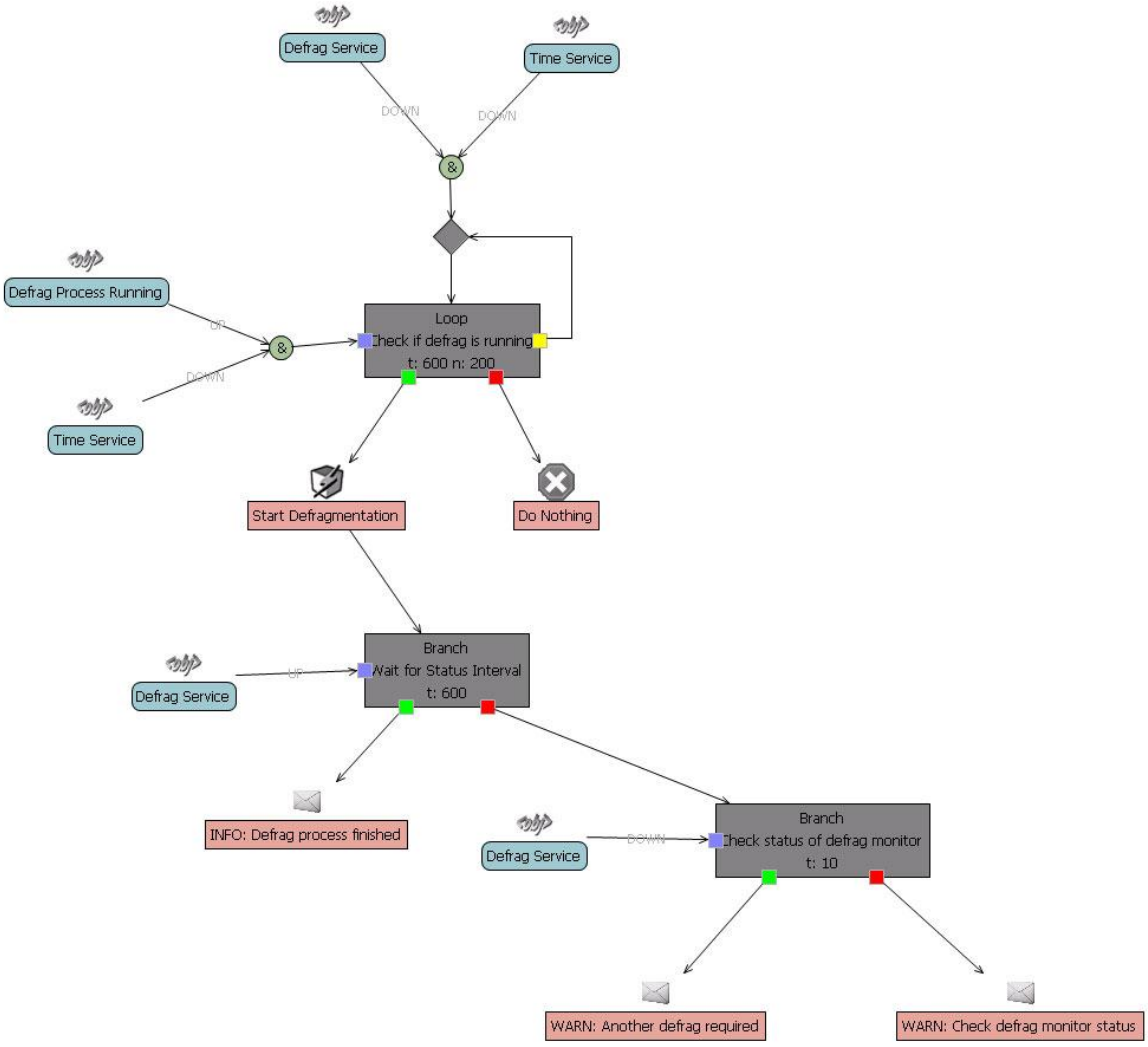


Automatic disk defragmentation

TASK: We need to defragment disks automatically. Process should not be run during working hours.

SOLUTION: For this we need two rule triggers. One is Defragmentation monitor and second is time service. Time service will make sure that defrag will not run during working hours. Once both monitors are DOWN, meaning partition requires defragmentation and it is not working hours, rule will start. First it needs to check if another defrag process is running. If it is rule will wait until other process finish before starting defragmenting partition. After defragmentation process finishes it will check status of monitor and send an e-mail depending on status of monitor.

RULE:

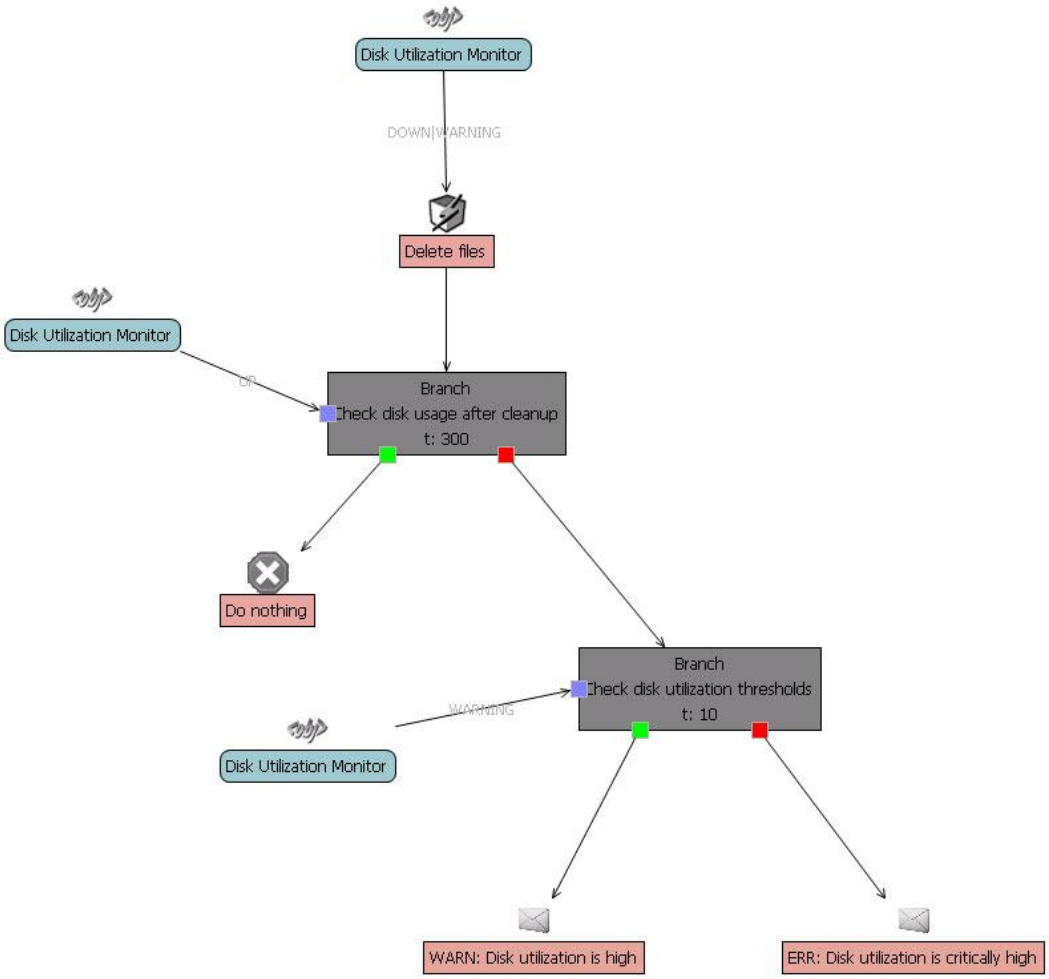


Delete files when disk usage gets high

TASK: When disk starts lacking disk space we usually delete certain files (old logs, temporary files, etc). We need to automate this.

SOLUTION: We have the monitor which checks disk utilization. On that monitor we can specify thresholds. When disk utilization gets over threshold we can trigger rule which automatically deletes those files and then afterwards it can inform us if disk usage is still high.

RULE:

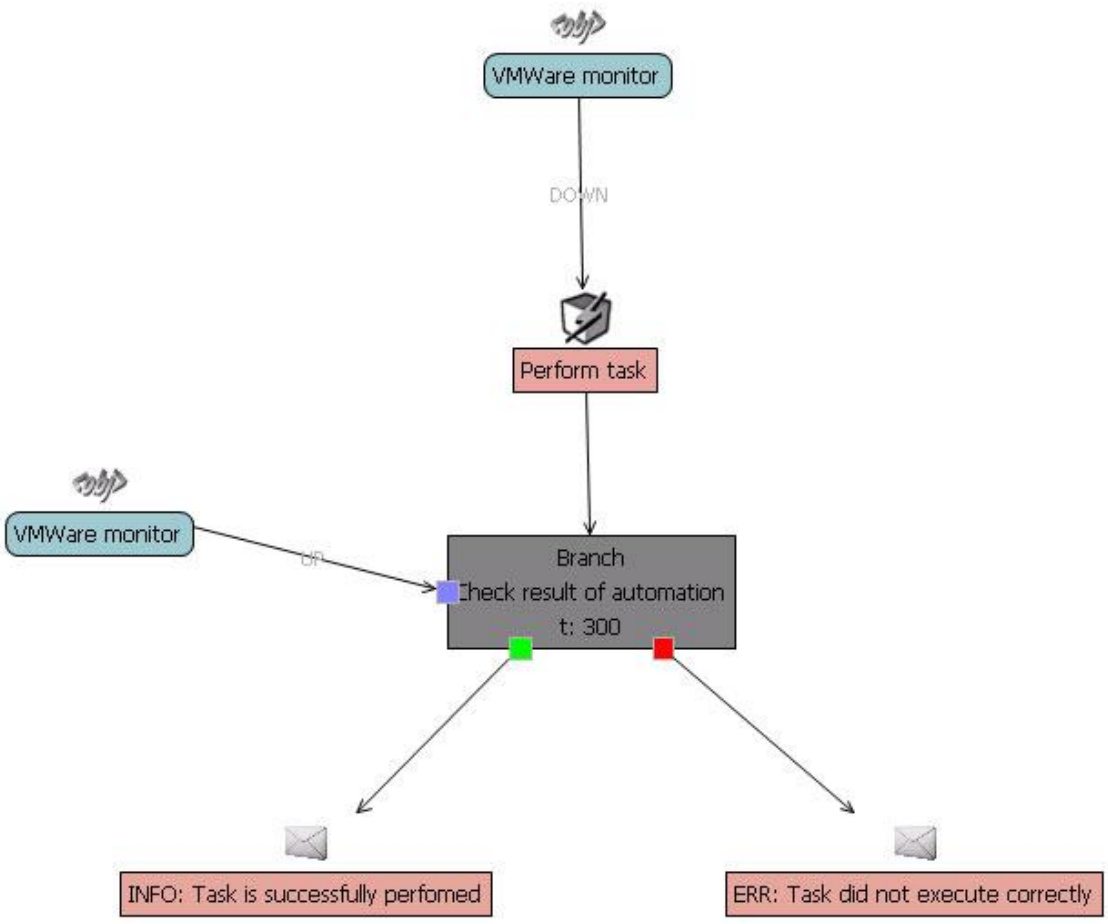


VMWare automation

TASK: We need to monitor and perform various automation tasks on VMWare (e.g. make snapshot, revert snapshot, etc.)

SOLUTION: There are many powershell scripts which lets you monitor and automate VMWare tasks. What we do is creating custom monitor and use such scripts to obtain status. Then we use that monitor for the rule trigger that will perform automation.

RULE:

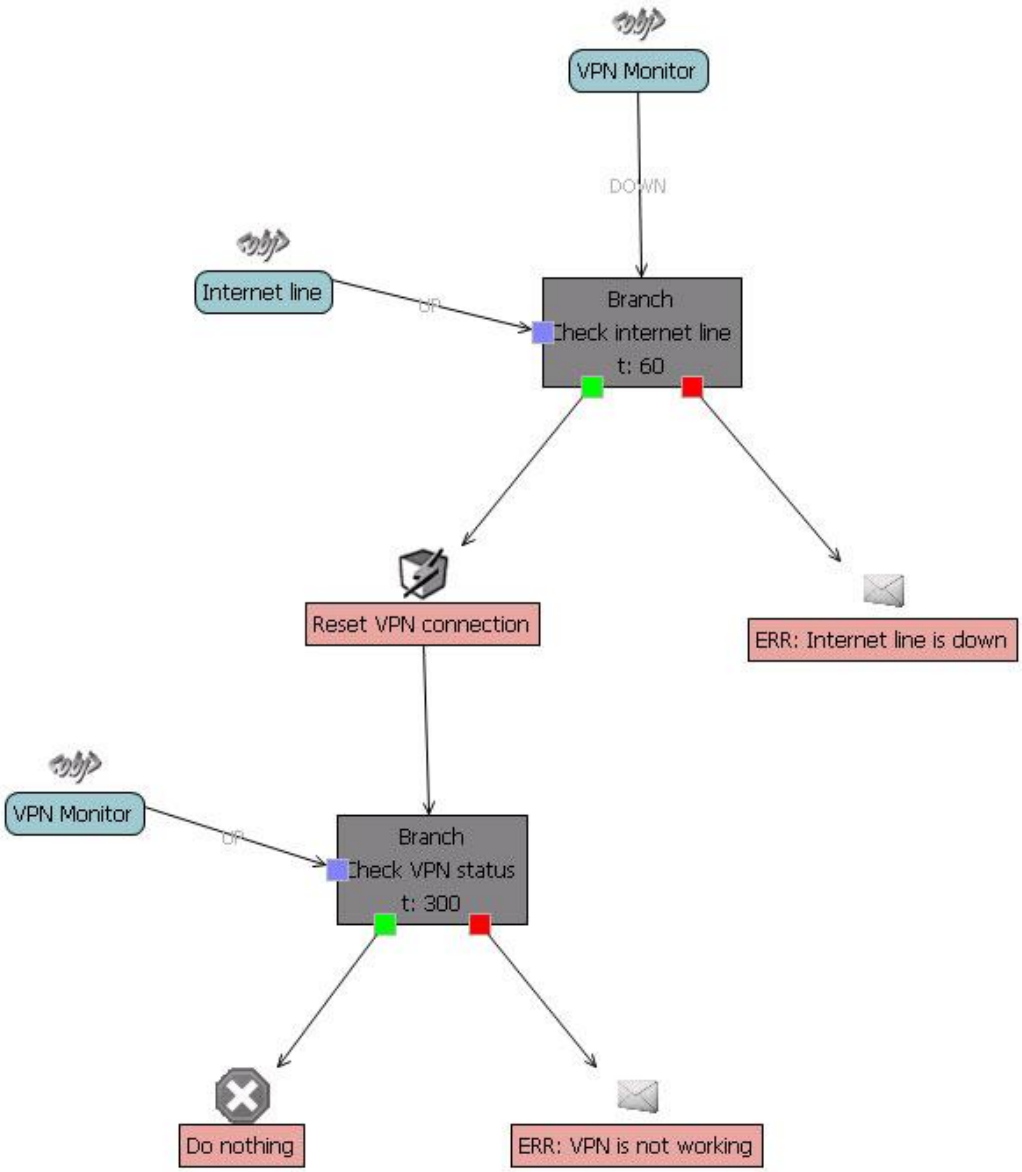


Notify when VPN is not available

TASK: We need to monitor VPN connections and when they are not working to be informed.

SOLUTION: We are able to monitor VPN status directly on router using SNMP. We can use such monitor as a rule trigger. Once VPN is down first we need to check if internet line is fine and if it is then we can try to restart VPN connection. At the end we check if restart helped.

RULE:

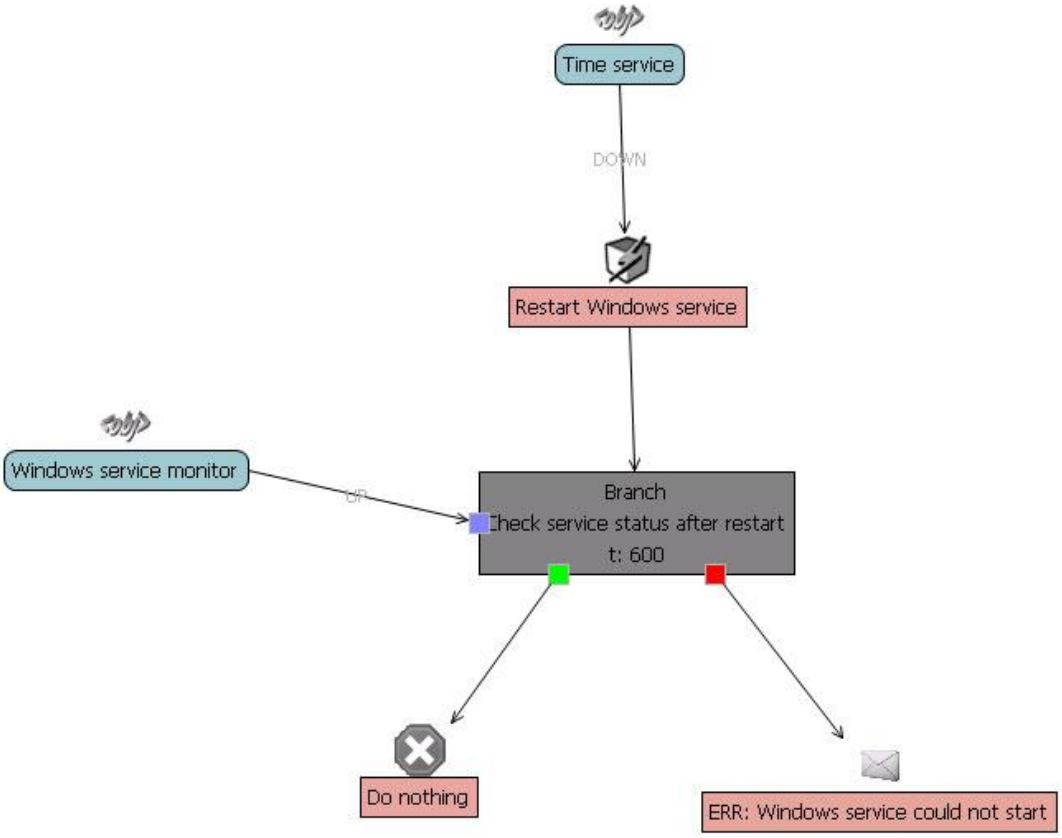


Periodically restart Windows services

TASK: We need to periodically restart Windows services. In case service does not restart correctly we need to be informed.

SOLUTION: We can use time service in order to trigger rule periodically. Once rule is triggered it will restart service. After restart it checks if service is UP and sends an e-mail in case of any issues.

RULE:

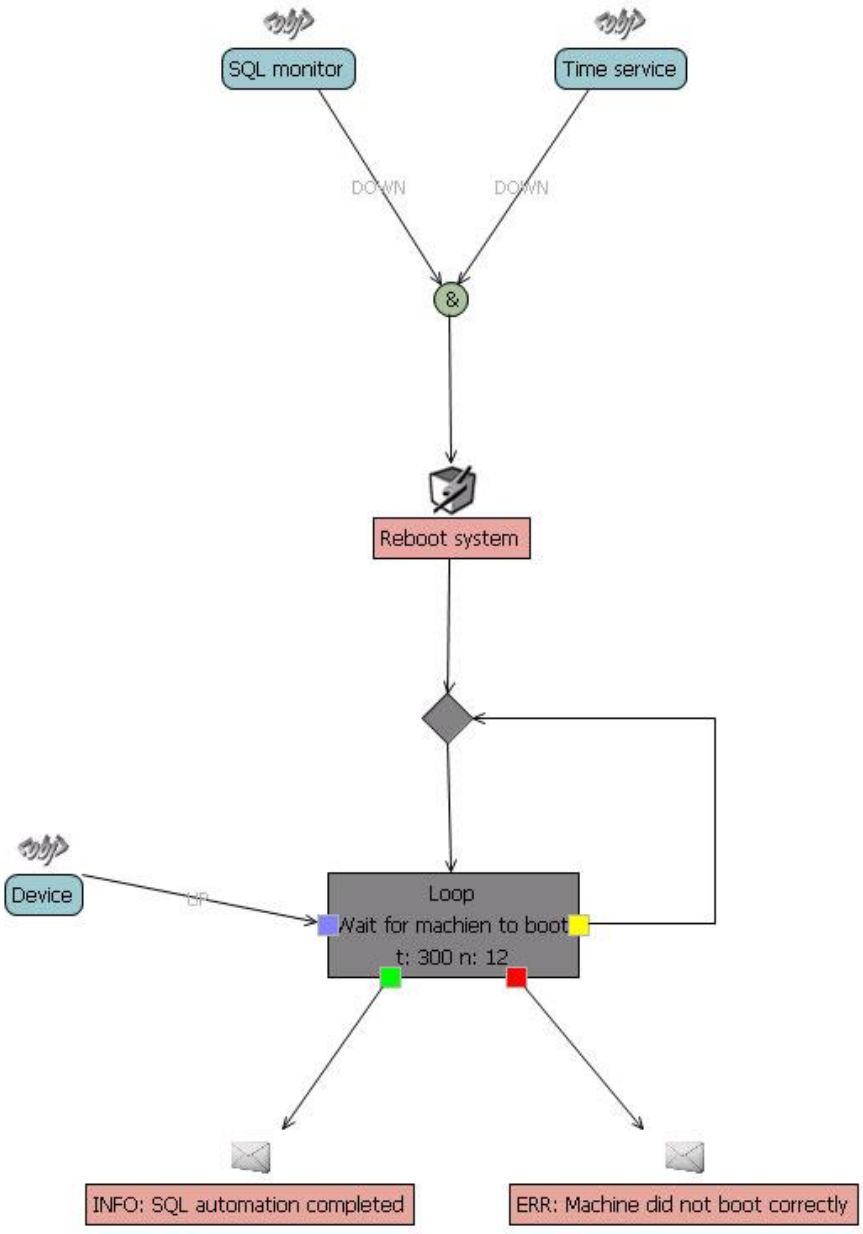


Check SQL tables for new entries

TASK: We need to check if there are new entries in specific table in SQL in last X hours. If there is no new entries during that timeframe we restart machine at specific time (e.g. after working hours). We would also like to be notified about this.

SOLUTION: We can create monitor which will check specific table for new entries during specified time period. We will use that monitor as a rule trigger. Since we cannot reboot machine during working hours we will use a second trigger which will be the time service (which will be in DOWN state after working hours). When both conditions are met, the rule will trigger and proceed with automation. At the end we check if machine boot correctly and send an e-mail.

RULE:

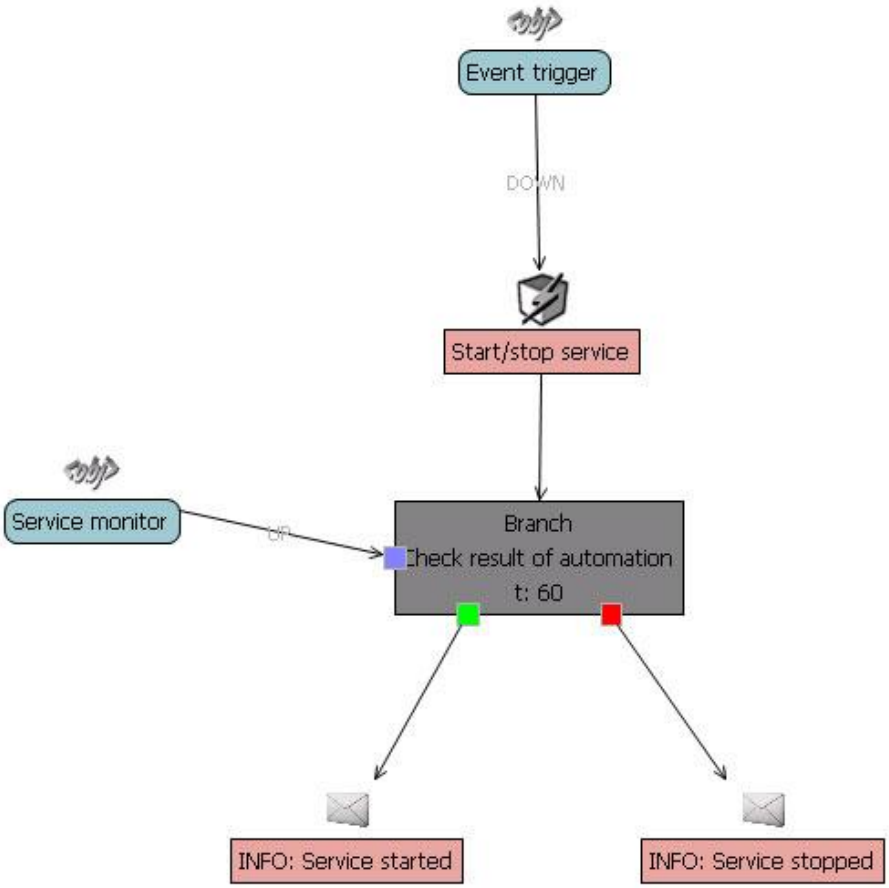


Automatic stop/start of Windows services based on different events

TASK: We need to start/stop Windows services depending on different events.

SOLUTION: For this we need first to create monitors for different events. Those monitors will be rule triggers. Once rule is triggered we start/stop Windows service depending on what we need to do in that case. At the end we check the result of automation and send info e-mail.

RULE:



Automatic Event log maintenance

TASK: Our event logs get large over time so they become quite hard to read. We would like to export event logs automatically once a week.

SOLUTION: For this we need the time service for setting the time when logs will be exported (e.g. on Saturday at 8 pm). Then we simply call command which will export event logs to file.

RULE: