Lab 06.1: Monitoring Introduction
IN719 Systems Administration

Introduction

Early in the semester I said that one of our aims as sysadmins is to always know the states of our servers. If something goes wrong we would like to notice it before our users do. Even better, if we're well informed about the states of our servers we can catch potential problems early before they degrade services. But of course we can't just watch our servers around the clock. Instead we set up automated monitoring systems and configure them to notify us when problems occur.

One very widely used example of a monitoring system is *Nagios*. You should have installed Nagios on your `mgmt` server when you did lab 5.2. If you have not completed that lab, do so right now. Confirm that the `nagios3` service is running on your server with the command `systemctl status nagios3` and start it if necessary.

1 The Nagios Web Dashboard

You can see what Nagios is monitoring by checking it's web dashboard. Use the Polytech's Citrix workspace to open a web browser that can access the internal network. Visit the web page at `http://<ip address of your server>/nagios3`. You will be prompted for a username (`nagiosadmin`) and a password that you set up as part of the previous lab.

Click the **Hosts** link on the left side menu. You should see two hosts being monitored, `localhost` (that was set up as part of the installed defaults) and your db server that you set up in the previous lab. The status of both should the "UP". Nagios monitors the host by simply pinging them and checking for the responses.

Next, click the **Services** link in the menu and look at the monitored services for `localhost`. You should see six things being monitored: Current Load, Current Users, Disk Space, Total Processes, SSH, and HTTP. The first four are properties of the local state of the machine while the last two are network services. For now we will focus on the network services.

2 Nagios Configuration

It's easy to check the status of services, like SSH, that are accessible over the network. The Nagios server simply tries the connect to the service over the network and tracks whether it succeeds. All of our servers run sshd, so we should check it on all of them. To do this, we will create *host* entries for each of our servers then we will create a *host group* containing the hosts that run sshd (all of them, in our case). Finally, we will create a *service* entry for our ssh service that describes how to check the service status.

Nagios configuration files are located in `/etc/nagiso3/conf.d`. The Nagios server will read any files in that directory that end in `.cfg`. If you look in that directory you will see some files in there. You should look at those files, but we won't work with them directly. Instead we will work with Puppet resources that manage Nagios configuration elements and writes the needed files. We will explore how to do this in today's lab.