Nagios

Relatório da configuração do sistema de monitorização de serviços, servidores e dispositivos de rede Nagios

LAPR5/ASIST – DEI – ISEP 2012/2013

1100554 – Bruno Cunha – 3DD

1100592 – Hugo Dias – 3DD

1101340 – Leniker Gomes – 3DD

1100638 – Mário Queirós – 3DD

1100677 – Tiago Queirós – 3DD

Máquina Linux: uvm035.dei.isep.ipp.pt

Máquina Windows: wvm035.dei.isep.ipp.pt

Nagios

Relatório da configuração do sistema de monitorização de serviços, servidores e dispositivos de rede Nagios

A vida de um administrador de sistema ficou mais descomplicada com a criação de sistemas de monitorização com notificações sempre que algum serviço ou servidor, que seja da sua responsabilidade (ou não).

O sistema usado no nosso trabalho foi o Nagios. Este sistema de monitorização bastante poderoso e não muito complicado de configurar consegue mostrar o estado da rede, serviços, servidores e dispositivos de rede.

Estrutura configuração Nagios

O Nagios é instalado na pasta "/etc/nagios3". Podemos construir os nossos próprios comando usando o ficheiro "commands.cfg". O ficheiro "Nagios.cfg" foi alterado para se proceder às configurações realizadas neste trabalho. As configurações alteradas foram as seguintes:

```
# You can specify individual object config files as shown below:
cfg_file=/etc/nagios3/objects/templates.cfg
# Definitions for monitoring a Windows machine
cfg_file=/etc/nagios3/objects/windows.cfg
cfg_file=/etc/nagios3/objects/sqlserver.cfg
# Definitions for monitoring a router/switch
cfg_file=/etc/nagios3/objects/switch.cfg
```

Existem estruturas chamadas "templates" onde será configurado o tipo de servidor a ser monitorizado. Estes templates são usados noutras estruturas, "host" para se saber como se proceder ao tipo de notificações, frequência de monitorização, quem contactar em caso de WARNING/CRITICAL.

```
####################
#  Template Swicth  #
####################
define host{
        name                    generic-switch  ; The name of this host template
        use                     generic-host    ; Inherit default values from the generic-host template
        check_period            24x7            ; By default, switches are monitored round the clock
        check_interval          5               ; Switches are checked every 5 minutes
        retry_interval          1               ; Schedule host check retries at 1 minute intervals
        max_check_attempts              10              ; Check each switch 10 times (max)
        check_command           check-host-alive        ; Default command to check if routers are "alive"
        notification_period     24x7            ; Send notifications at any time
        notification_interval   30              ; Resend notifications every 30 minutes
        notification_options    d,r             ; Only send notifications for specific host states
        contact_groups          admins          ; Notifications get sent to the admins by default
        register                        0               ; DONT REGISTER THIS - ITS JUST A TEMPLATE
        }
```

Fig. 1 – Exemplo de um template. Neste caso de um switch.

Existem já templates criados em "/etc/nagios3/conf.d/generic-host_nagios2.cfg", onde podemos adicionar mais ou retirar. Na nossa configuração também existe o ficheiro "/etc/nagios3/objects/templates.cfg" com templates criados por nós.

O ficheiro "/etc/nagios3/conf.d/generic-service_nagios2.cfg" contém o template para a estrutura dos serviços a serem usados nos comandos.

Já "/etc/nagios3/conf.d/services_nagios2.cfg" contém serviços predefinidos.

Em "/etc/nagios3/conf.d/localhost_nagios2.cfg" estão as definições dos serviços para monitorizar a nossa própria máquina.

Umas das partes principais são as notificações de serviços em falha. Logo é preciso configurar o tipo de notificação a ser enviada. O ficheiro "/etc/nagios3/conf.d/contacts_nagios2.cfg" contém a definição da estrutura que contém a informação para contactar o administrado do sistema. Nesta estrutura está o email e o tipo de notificação a ser enviada. Nesta configuração usamos notificação por email e SMS.

O definição dos comandos para envio de notificações por email e SMS encontra-se no ficheiro "/etc/nagios3/commands.cfg". Usando o comando Linux sendEmail é possível enviar uma notificação para o colocado no ficheiro de configuração dos contactos.

A notificação por SMS foi mais difícil de se conseguir colocar a funcionar correctamente. Como o envio de SMS não é gratuito procurar serviços que disponibilizassem créditos para teste. Encontramos o serviço http://www.smsmail.com que oferece 10 créditos para envio de SMS grátis. A utilização deste serviço é bastante simples, bastando enviar um email para 351xxxxxxxxx@smsmail.com onde x é o número para o qual o administrador quer ser contactado. Este número de telemóvel encontra-se no ficheiro "/etc/nagios3/resource.cfg" no campo $USER8$. O email de remetente terá de ser o email que foi usado

na criação da conta no site SMSMail. O ficheiro "resource.cfg" contém outras definições de variáveis a serem usadas sempre que seja necessário. É o caso do "$USER1$=/usr/lib/nagios/plugins" que se traduz onde se pode encontrar os plugins para se usar nos comandos.

Comutadores de Rede

(/etc/nagios3/objects/switch.cfg /etc/nagios3/objects/windows.cfg)

O Nagios suporta plugins para completar os já existentes. Para se conseguir resolver o problema de monitorizar a porta de um switch, tivemos de usar o plugin "check_snmp_int.pl". O comando usa o protocolo SNMP.

O comando usado para monitorizar as portas de switchs foi o seguinte:

```
####################
#  Switch sw2626a  #
####################
define command {
        command_name    check_snmp_m
        command_line    /usr/bin/perl $USER1$/check_snmp_int.pl -H $HOSTADDRESS$ -C public -k -u -n $ARG1$ -w 80,80 -c 90,90
        }
```

Fig. 1

$HOSTADDRESS$ - IP do switch

$ARG1$ - Nome da porta a monitorizar

-w 80,80 – Quando o tráfego atingir 80% da capacidade total da porta, o Nagios irá enviar uma notificação do tipo WARNING

-c 90,90 - Quando o tráfego atingir 90% da capacidade total da porta, o Nagios irá enviar uma notificação do tipo CRITICAL

A definição do host e do serviço para usar o comando acima referido foi a seguinte:

```
##################
#  Host sw2626a  #
##################
define host {
        use             generic-switch
        host_name       sw2626a.dei.isep.ipp.pt
        alias           HP ProCurve Switch 2626
        address         172.22.3.40
        }

#########################
#  Interface Uplink 25  #
#########################
define service {
        use                     generic-service
        host_name               sw2626a.dei.isep.ipp.pt
        service_description     TRAFEGO - Porta 25
        check_command           check_snmp_m!25
        contact_groups          admins
        }
```

Fig. 2

É passado como parâmetro no comando "check_snmp_m", 25, o número da porta a monitorizar.

Decidimos também monitorizar a porta de rede " VMware Accelerated AMD PCNet Adapter" no servidor Gandalf.

```
#########################
#  Interface Rede Gandalf #
#########################
define command{
       command_name    check_nt_sqlserver
       command_line    /usr/bin/perl $USER1$/check_snmp_int.pl -H 193.136.62.27 -C public -n "VMware Accelerated AMD PCNet Adapter" -w 80,80 -c 90,90
       }
```

Fig. 3 - Definição do comando

```
##################
#  Host Gandalf  #
##################
define host{
        use             gandalf
        host_name       gandalf.dei.isep.ipp.pt
        alias           GANDALF.dei.isep.ipp.pt
        address         193.136.62.27
        }
```

Fig. 4 – Definição do host

```
####################
#  Interface rede  #
####################
define service{
        use                     generic-service
        host_name               gandalf.dei.isep.ipp.pt
        service_description     Trafego Interface Rede
        check_command           check_nt_sqlserver
        }
```

Fig. 5 – Definição do serviço

$HOSTADDRESS$ - IP do servidor Gandalf

-w 80,80 – Quando o tráfego atingir 80% da capacidade total da porta, o Nagios irá enviar uma notificação do tipo WARNING

-c 90,90 - Quando o tráfego atingir 90% da capacidade total da porta, o Nagios irá enviar uma notificação do tipo CRITICAL

SSH

(/etc/nagios3/conf.d/host-gateway_nagios3.cfg)

Outro dos serviços a monitorizar é um dos servidores SSH disponíveis no Departamento de Informática.

Para isso usamos a seguinte configuração do host e serviço:

```
#############
#  SSH Dei  #
#############
define host {
        host_name               ssh3.dei.isep.ipp.pt
        alias                   ssh3.dei.isep.ipp.pt
        address                 193.136.62.25
        use                     generic-host
        contact_groups          admins
        }

#############
#  SSH Dei  #
#############
define service {
        use                     generic-service
        host_name               ssh3.dei.isep.ipp.pt
        service_description     SSH - SSH3.dei.isep.ipp.pt
        check_command           check_ssh
        contact_groups          admins
        }
```

Fig. 6 – Definição serviço e host

O comando usado foi o "check_ssh", que não requer que sejam passados parâmetros para proceder à monitorização do servidor SSH.

DEI, Portal, Moodle e Google

(/etc/nagios3/conf.d/host-gateway_nagios3.cfg)

DEI

Foi-nos pedido que sejam monitorizados os serviços HTTP/HTTPS do servidor WEB do DEI, ISEP (Portal e Moodle) e de um servidor externo (escolhemos o sugerido, Google).

```
##############
#  Host Dei  #
##############
define host {
        host_name               dei.isep.ipp.pt
        alias                   dei.isep.ipp.pt
        address                 193.136.62.2
        use                     generic-host
        contact_groups          admins
        }

##############
#  HTTP Dei  #
##############
define service {
        use                     generic-service
        host_name               dei.isep.ipp.pt
        service_description     HTTP - DEI.isep.ipp.pt
        check_command           check_http
        contact_groups          admins
        }

###############
#  HTTPS Dei  #
###############
define service {
        use                     generic-service
        host_name               dei.isep.ipp.pt
        service_description     HTTPS - DEI.isep.ipp.pt
        check_command           check_https
        contact_groups          admins
        }
```

Fig. 7 – Definição do host e dos serviços HTTP e HTTPS do servidor WEB do DEI

Portal

No caso do Portal e do Moodle foi preciso de arranjar uma solução alternativa ao "check_http"/"check_https" para contornar a rejeição de pedidos ping a estes servidores.

Devido a este problema, resolvemos tentar realizar um check_tcp à porta 80 e 443 (HTTP e HTTPS, respectivamente) destes servidores. A qual retornou uma resposta positiva. Isto deve-se ao facto de os servidores estarem sempre a "ouvir" na porta 80/443 para quem faz pedidos HTTP, logo, caso os servidores não estejam activos, não vão responder aos pedidos na porta 80/443, por isso irá retornar um erro. Este erro será tratado pelo Nagios e serão enviadas notificações.

```
##################
#  Host Portal   #
##################
define host {
        host_name               portal.isep.ipp.pt
        alias                   portal.isep.ipp.pt
        address                 193.136.60.7
        use                     host-tcp
        contact_groups          admins
        }

##################
#  HTTP Portal   #
##################
define service {
        use                     generic-service
        host_name               portal.isep.ipp.pt
        service_description     HTTP - PORTAL.isep.ipp.pt
        check_command           check_tcp_80
        contact_groups          admins
        }

##################
#  HTTPS Portal   #
##################
define service {
        use                     generic-service
        host_name               portal.isep.ipp.pt
        service_description     HTTPS - PORTAL.isep.ipp.pt
        check_command           check_tcp_443
        contact_groups          admins
        }
```

Fig. 8 – Definição host e serviços HTTP e HTTPS do Portal

Moodle

```
#################
#  Host Moodle  #
#################
define host {
        host_name               moodle.isep.ipp.pt
        alias                   moodle.isep.ipp.pt
        address                 193.136.60.61
        use                     host-tcp
        contact_groups          admins
        }

#################
#  HTTP Moodle  #
#################
define service {
        use                     generic-service
        host_name               moodle.isep.ipp.pt
        service_description     HTTP - moodle.isep.ipp.pt
        check_command           check_tcp_80
        contact_groups          admins
        }

##################
#  HTTPS Moodle  #
##################
define service {
        use                     generic-service
        host_name               moodle.isep.ipp.pt
        service_description     HTTPS - moodle.isep.ipp.pt
        check_command           check_tcp_443
        contact_groups          admins
        }
```

Fig. 9 – Definição host e serviços HTTP e HTTPS do Portal

Google

No caso do servidor WEB do Google não foi preciso realizar "check_tcp". Foi possível usar o "check_http"/"check_https".

```
#################
#  Host Google #
#################
define host {
        host_name               www.google.pt
        alias                   www.google.pt
        address                 74.125.227.88
        use                     generic-host
        contact_groups          admins
        }

##################
#  HTTP Google  #
##################
define service {
        use                     generic-service
        host_name               www.google.pt
        service_description     HTTP - www.GOOGLE.pt
        check_command           check_http
        contact_groups          admins
        }

###################
#  HTTPS Google  #
###################
define service {
        use                     generic-service
        host_name               www.google.pt
        service_description     HTTPS - www.GOOGLE.pt
        check_command           check_https
        contact_groups          admins
        }
```

Fig. 10 – Definição host e serviços HTTP e HTTPS do Portal

Servidor Windows

(/etc/nagios3/objects/windows.cfg)

O enunciado do trabalho refere para monitorizar o servidor Windows que vai ser usado o website e web services. Foi-nos pedido para verificar a utilização do CPU e discos, o estado dos serviços HTTP, o serviço SQLServer localizado no servidor Gandalf e como acima referido o trafego da interface de rede do servidor Windows.

```
##################
#  Host WVM035  #
##################
define host{
        use             windows-server
        host_name       WVM035.dei.isep.ipp.pt
        alias           Windows Server
        address         172.31.101.35
        }
```

Fig. 11 – Definição do host do servidor Windows

Utilização CPU

```
##############
#  CPU Load  #
##############
define service{
        use                     generic-service
        host_name               WVM035.dei.isep.ipp.pt
        service_description     CPU Load
        check_command           check_nt_m!CPULOAD!-l 5,80,90
        }
```

Fig.12 – Definição do serviço para monitorização da utilização do CPU

É passado como parâmetro o valor 80, para o aviso de WARNING e 90 para o de CRITICAL, assim como o serviço a ser monitorizado (CPULOAD).

Utilização Discos

```
################
#  Disk Usage  #
################
define service{
        use                     generic-service
        host_name               WVM035.dei.isep.ipp.pt
        service_description     C:\ Drive Space
        check_command check_nt_m!USEDDISKSPACE!-l c -w 75 -c 90
        }
```

Fig. 13 – Definição do serviço de monitorização da utilização do CPU

O comando está configurado para notificar com estado de WARNING quando disco tiver 75% da quota total ocupada e com estado CRITICAL quando esta quota for superior a 90%, assim como o serviço a monitorizar (USEDISKSPACE).

Estado dos Serviços HTTP

```
#################
#  HTPP WVM035  #
#################
define service{
        use                     generic-service
        host_name               WVM035.dei.isep.ipp.pt
        service_description     WVM035 - HTTP
        check_command           check_http
        }
```

Fig. 14 – Definição do serviço de monitorização dos serviços http

Serviços extras no Servidor Windows wvm035

Utilização da Memória RAM

```
##################
#  Memory Usage  #
##################
define service{
        use                     generic-service
        host_name               WVM035.dei.isep.ipp.pt
        service_description     Memory Usage
        check_command           check_nt_m!MEMUSE!-w 80 -c 90
        }
```

Fig. 16 – Definição do serviço de monitorização da utilização da memória RAM

São passados como parâmetro os valores –w 80 para o estado de WARNING e o valor –c 90 para o estado de CRITICAL e o serviço a monitorizar pelo "check_nt_m" (MEMUSE).

Uptime e versão do cliente NSClient++

```
################################
#  Client Version  NSClient++  #
################################
define service{
        use                     generic-service
        host_name               WVM035.dei.isep.ipp.pt
        service_description     Client Version
        check_command           check_nt_m!CLIENTVERSION
        }

############
#  Uptime  #
############
define service{
        use                     generic-service
        host_name               WVM035.dei.isep.ipp.pt
        service_description     Uptime
        check_command           check_nt_m!UPTIME
        }
```

Fig. 17 – Definição dos serviços de Uptime da versão do cliente NSClient++

```
####################
#  Maquina WVM035  #
####################
define command{
        command_name    check_nt_m
        command_line    $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s gaivota -v $ARG1$ $ARG2$
        }
```

Fig. 15 – Definição do comando "check_nt_m" para ser usado na monitorização do nosso servidor (uvm035)

O cliente NSClient++ está à escuta na porta 12489, como mostra na imagem em cima (-p 12489) e sendo preciso password para se conseguir aceder a estes serviços (-s gaivota). Recebe como parâmetro os valores passados no ficheiro de configuração do serviço ($ARG1$ e $ARG2$).

SQL Server – Gandalf

(/etc/nagios3/objects/sqlserver.cfg)

O seguinte ponto a monitorizar é o servidor SQLServer – Gandalf. Decidimos para este caso verificar a porta 1433 que é porta para se realizam os pedidos ao SQLServer.

Para isso fizemos o seguinte:

```
##################
#  Host Gandalf  #
##################
define host{
        use             gandalf
        host_name       gandalf.dei.isep.ipp.pt
        alias           GANDALF.dei.isep.ipp.pt
        address         193.136.62.27
        }

##############
#  HTTP/TCP  #
##############
define service{
        use                     generic-service
        host_name               gandalf.dei.isep.ipp.pt
        service_description     SQL Service Port 1433
        check_command           check_tcp_1433
        }
```

Fig. 18 – Definição do host e do serviço para monitorizar a porta 1433

```
#################################
#  TCP Portal/Moodle Porta 1433  #
#################################
define command{
        command_name    check_tcp_1433
        command_line    $USER1$/check_tcp -H $HOSTADDRESS$ -p 1433
        }
```

Fig. 19 – Definição do comando "check_tcp_1433" no ficheiro commands.cfg