LINUX

VPN

#Apt-get install openvpn openssl

#mkdir /etc/openvpn/ssl-cert

#cp –rp /usr/share/doc/openvpn/examples/easy-rsa/2.0/\* /etc/openvpn/easy-rsa

#mkdir /etc/openvpn/easy-rsa/keys

#source vars

#./clean-all

#./build-ca

#./build-key-server NOME\_SERVIDOR

#./build-key usuariodavpn

#./build-dh

#openvpn –genkey –secret chave-key

Mkdir /etc/openvpn/keys

Cp –a dh1024.pem ca.crt NOME\_SERVIDOR.crt NOME\_SERVIDOR.key chave.key

Copiar arquivos pros clientes dh1024.pen ca.crt usuariovpn.crt e .key e chave.key, usar arquivos de clientes e server que estão no docs da vpn!

APACHE

PHP

<\br> //quebra de linha

<?php

$Date = date (“d/m/Y”);

$Hour= date(“h:i:s”);

echo $Date;

echo “</br>”;

echo $Hour;

?>

Autenticação do apache

Primeiramente habilite o módulo ldap no apache2. (Teste efetuado)

root@debian:~# a2enmod authnz\_ldap

E reinicie o apache.

root@debian:~# /etc/init.d/apache2 restart

Em seguida, ajuste o apache.

root@debian:~# vi /etc/apache2/sites-avaliable/default

<Directory /var/www>

Options Indexes FollowSymLinks MultiViews

AllowOverride None

Order allow,deny

allow from all

AuthType Basic

AuthBasicProvider ldap

AuthzLDAPAuthoritative off

AuthName "Acesso Restrito"

AuthLDAPURL ldap://192.168.8.2:3268/dc=vinicius,dc=com?sAMAccountName

AuthLDAPBindDN cn=apache,ou=usuarios,dc=vinicius,dc=com

AuthLDAPBindPassword 1@asdfg

Require valid-user

#Require peao

</Directory>

ARQUIVOS

apt-get install cifs-utils

nano /etc/rc.local

-> Adicionar a linha

mount.cifs //10.0.230.253/suporte /root/rede -o user=suporte,pass=1@asdfg

nano /etc/crontab

-> Adicionar a linha

# m h dom mon dow user command

\*/1 \* \* \* \* root rm -Rf /root/rede; cp -Rf /home/webmaster /root/rede

opções de comando

tar -cf webmaster.tar /home/webmaster ; gzip -9 webmaster.tar ; mv webmaster.tar.gz /root/rede

Cacti

Instalando ferramenta SNMP para monitoramento de equipamento

#apt-get install snmp snmpd mysql-server apache2 libapache2-mod-php5 php5 php5-snmp libnet-snmp-perl libsnmp15 cacti

Será pedido a senha do root do MySQL, escolha uma de sua preferência e guarde-a pois

vamos utilizar na configuração do Cacti.

Agora iremos proceder com a configuração final do Cacti para que ele possa estar

disponível para gerar os gráficos de uso dos ativos de rede que queremos monitorar.

Criando o Virtual Host para o CACTI

# cp /etc/cacti/apache.conf >> /etc/apache2/sites-available/default

Acesse http://IP\_SERVIDOR\_CACTI/cacti

Siga os passos abaixo para concluir a configuração:

1- Clique em NEXT;

2- Escolha a opção NEW INSTALL;

3- Clique em FINISH (Caso todos os testes de compatibilidade tenha dado Ok);

4- Faça o login com:

-> User: admin

-> Pass: admin

OBS.: Em seguida teremos que alterar a senha do admin.

Por fim, vamos adicionar uma regra no crontab para fazer a coleta de informações a cada 5 minutos

#crontab -e \*/5 \* \* \* \* /usr/share/cacti/site/poller.php

#############################

Cliente Linux

#############################

Cliente CISCO

Cisco\_device#conf t

Cisco\_device(config)#snmp-server community "your\_community" RO

Uma pequena mais segura configuração:

Cisco\_device#conf t

Cisco\_device(config)#snmp-server community "your\_community" RO 1

Cisco\_device(config)#access-list 1 permit "snmp\_server\_IP\_address"

#apt-get install nagios3

#cat /etc/nagios3/apache2.conf >> /etc/apache2/sites-avalaible/default

adicionando dispositivos

#cp /etc/nagios3/conf.d/localhost\_nagios2.cfg /etc/nagios3/conf.d/nome\_maquina.cfg

#nano /etc/nagios3/conf.d/nome\_maquina.cfg

CTR+\ localizar localhost -> substituir pelo hostname do dispositivo e no IP botar o IP do dispositivo

10.0.230.240/nagios3

nagios3admin

senha

adicionando serviços, roteadores e switchs

depois de copiar o localhost pra cada um dos hosts

ir em /etc/nagios3/conf./services\_nagios2.cfg

ex pra cada serviço, roteador ou switch

DNS

define service {

hostgroup\_name DNS-servers

service\_description DNS

check\_comand check\_dns

use generic-service

notification\_interval 0; set ...........

}

Roteador

define service {

hostgroup\_name Router

service\_description Router

check\_comand check-router-alive

use generic-service

notification\_interval 0; set ...........

}

O check\_command pode ser verificado na interface web do nagios, em configurações, check commands.

Adicionar Grupo de Hosts

ir em /etc/nagios3/conf./hostgroups\_nagios2.cfg

ex:

define hostgroup {

hostgroup\_name Router (ou DNS-server ou HTTP-server)

alias Router / Cisco (mesmo de cima)

members nome\_dispositivos

}

o Nome que ir no arquivo cfg do dispositivo ou host, é o mesmo que vai em members

Diretorio das imagens: /usr/share/nagios3/htdocs/images/logo

Botar icones no mapa dos hosts no arquivo nome\_arquivo.cfg que é criado pra cada host adicionar no final:

define hostextinfo {

host\_name nome\_da\_maquina (o que foi substituido no lugar do localhost)

icon\_image nome\_da\_imagem.png

icon\_image\_alt Grupo (ex: Servidores windows)

statusmap\_image nome\_da\_imagem.png

vrml\_image nome\_da\_imagem.png

}

usuario nagiosadmin

FreeRadius

OBS: Nastype é o tipo de autenticação de radius (cisco)

e shortname é o hostname do roteador, arbab no exemplo é o usuario que ele criou

o arquivo users em /etc/freeradius/users é onde vai ser criado os usuarios que podem usar o radius

OBS: O SO ONDE VAI ESTAR O PUTTY TEM QUE TA NA MESMA FAIXA DE IP DO ROTEADOR

No linux

#sudo apt-get install freeradius

#cd /etc/freeradius

#nano clients.conf

adicionar

client 192.168.179.152 { #IP do roteador

secret = secretkey -> password do roteador (será o mesmo que o grupo de radius utilizará pra autenticar)

nastype = cisco

shortname = hostname\_roteador

}

#sudo nano users -> arquivo onde será configurado os usuarios que acessarão via radius o roteador cada usuario terá a configuração abaixo

arbab Cleartext-Password := "password" #senha do usuario

Service-Type = NAS-Prompt-User,

Cisco-AVPair = "shell:priv-lvl=15" #privilegio de acesso

arbab é o nome de usuario que vai logar

restart o radius

#sudo /etc/init.d/freeradius restart

ROTEADOR

Secretkey é o password configurado no clients.conf no linux e server private é o ip do linux

#username BackupAdmin privilege 15 secret 5 $1$qLGb$VQ6BdqCEpzGZqPeC779Uh1

#conf t

#aaa new-model

#aaa group server radius RadiusGrp

#server-private 10.0. auth-port 1812 acct-port 1813 key secretkey

#exit

#ip domain-name xxx

#hostname xxx -> mesmo configurado no clients.conf

#crypto key generate rsa

#aaa authentication login default local group RadiusGrp

#aaa authorization exec default local group RadiusGrp

#aaa accounting exec default start-stop group RadiusGrp

#aaa accounting system default start-stop group RadiusGrp

#ine vty 0 4

#transport input telnet ssh

#login authentication default

VLAN

# apt-get install vlan

para ativar o modulo 8021q permanentemente

# echo 8021q >> /etc/modules

Para ativar o modulo 8021q sem reiniciar

#modprobe 8021q

Para testar(tem que retornar o numero do precesso)

#lsmod | grep 8021q

No arquivo /etc/network/interfaces

...

auto vlan2

iface vlan2 inet static

address 192.168.2.1

netmask 255.255.255.0

vlan-raw-device eth0

...

TRIPWIRE

# aptitude install tripwire (botar tudo em sim e botar os passwords)

editar o arquivo #nano /etc/tripware/twpol.txt

Apagar todos os comentarios das linha de cima e deixar apartir de section global e depois apagar tudo abaixo de sig\_hi = 100 ou seja o binaries pra frente e acrescentar os diretorios que pede pra ele analisar conforme abaixo

Após variaveis de configuração adicionar: [ HIGH - MED - LOW ]

(

rulename = "Sites do Debian", #Nome que vai aparecer no log

severity = $(SIG\_MED) #Nivel de mudança dos arquivos, critical medio

)

{

/var/www/ -> $(SEC\_CONFIG) ;

}

/var/www diretorio e sec config é o tipo de arquivo a ser analisado

# /usr/sbin/twadmin -m P /etc/tripwire/twpol.txt

# /usr/sbin/tripwire -m i

O primeiro verifica se o arquivo esta certo e o segundo comando gera a base de dados

# tripwire --check # vai analisar o arquivo e gerar um relatorio

# tripwire -m u -Z low -r /var/lib/tripwire/report/nome\_do\_server-timestamp.twr

esse comando é pra ver os relatorios

o diretorio /var/lib/tripwire/report/ é onde vai estar os relatorios que foi gerado com o nome da maquina e a data.