Laboratório - Configurar Gerenciamento de Resiliência Cisco IOS e Relatórios

Topologia

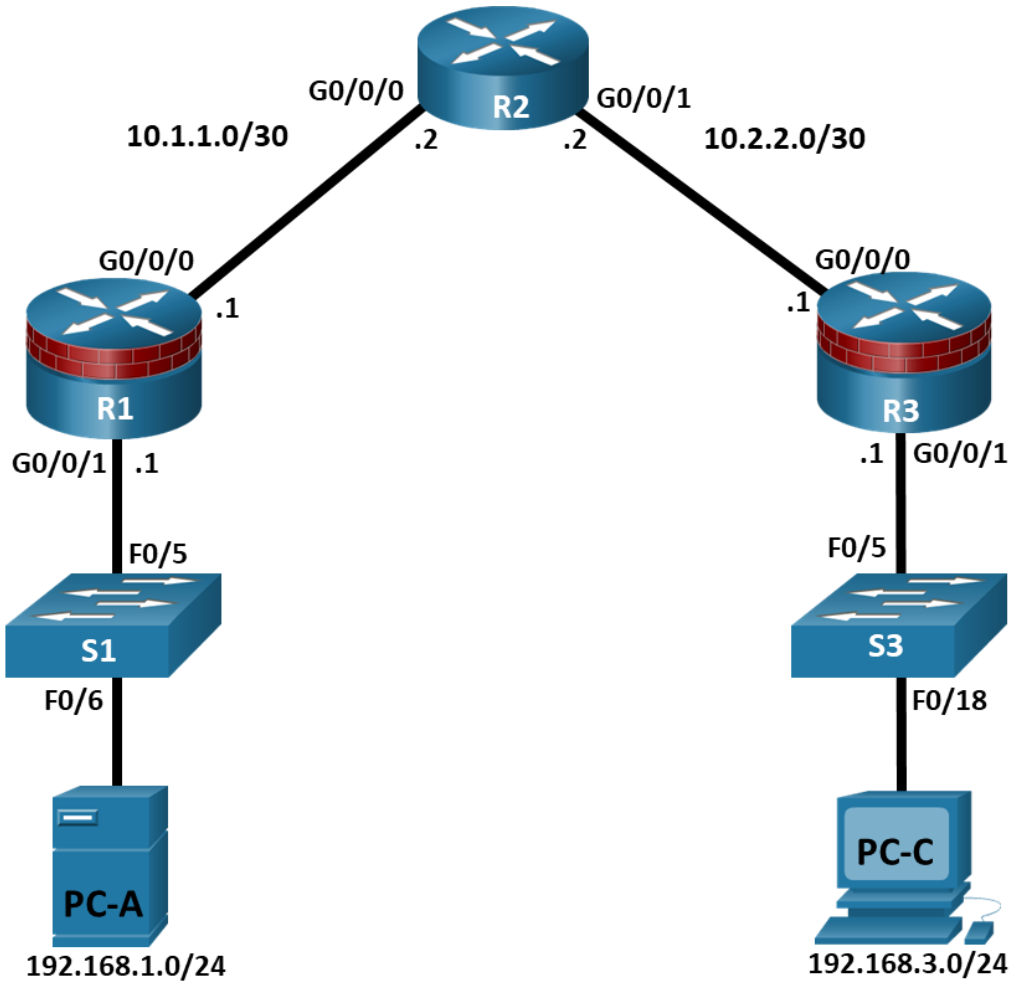

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de Sub-Rede	Gateway padrão	Porta do Switch
R1	G0/0/0	10.1.1.1	255.255.255.252	N/D	N/D
	G0/0/1	192.168.1.1	255.255.255.0	N/D	S1 F0/5
R2	G0/0/0	10.1.1.2	255.255.255.252	N/D	N/D
	G0/0/1	10.2.2.2	255.255.255.252	N/D	N/D
R3	G0/0/0	10.2.2.1	255.255.255.252	N/D	N/D
	G0/0/1	192.168.3.1	255.255.255.0	N/D	S3 F0 / 5
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objetivos

Parte 1: Implementar as Configurações Básicas do Dispositivo

Parte 2: Configure a segurança SNMPv3 usando uma ACL.

Parte 3: Configure um roteador como uma fonte de tempo sincronizado para outros dispositivos usando NTP.

Parte 4: Configurar o suporte a syslog em um roteador.

Histórico/Cenário

O roteador é um componente crítico em qualquer rede. Controla o movimento de dados dentro e fora da rede e entre dispositivos dentro da rede. É particularmente importante proteger os roteadores de rede porque a falha de um dispositivo de roteamento pode fazer seções da rede ou toda a rede, inacessível. Controlando o acesso a roteadores e a ativação de relatórios em roteadores é fundamental para a segurança de rede e deve fazer parte de uma política de segurança abrangente.

Neste laboratório, você criará uma rede multi-roteador e configurará os roteadores e os hosts. Você configurará o suporte SNMP, NTP e syslog para monitorar as alterações na configuração do roteador.

Nota: Os roteadores usados com laboratórios hands-on são Cisco 4221 com a versão 16.9.6 do Cisco IOS XE (imagem universersalk9). Os switches usados nos laboratórios são Cisco Catalyst 2960+ com a versão Cisco IOS 15.2 (7) (imagem lanbasek9). Outros roteadores, switches e versões do Cisco IOS podem ser usados. De acordo com o modelo e a versão do Cisco IOS, os comandos disponíveis e a saída produzida poderão variar em relação ao que é mostrado nos laboratórios. Consulte a Tabela de resumo de interfaces dos roteadores no final do laboratório para saber quais são os identificadores de interface corretos.

Nota: Antes de começar, verifique se os roteadores e os comutadores foram apagados e não têm configurações de inicialização.

Recursos necessários

- 3 roteadores (Cisco 4221 com a Cisco Xe Release 16.9.6 Imagem universal ou comparável com uma licença de pacote de tecnologia de segurança)
- 2 switches (Cisco 2960+ com lançamento do Cisco IOS 15.2 (7) imagem lanbasek9 ou comparável)
- Nota: Antes de Achar, Verifique SE OS Roteia e OS Comutadores Foram Apagados e Não têm configurações de inicialização.
- Cabos de console para configurar dispositivos de rede Cisco
- Cabos ethernet conforme mostrado na topologia

Instruções

Parte 1: Implementar as Configurações Básicas do Dispositivo

Nesta parte, configure a topologia da rede e configure as configurações básicas, como endereços IP da interface.

Etapa 1: Conectar a rede.

Anexar os dispositivos, conforme mostrado no diagrama de topologia e cabo conforme necessário.

Etapa 2: Defina as configurações básicas de cada Roteador.

a. Use o console para se conectar ao roteador e ative o modo EXEC privilegiado.

```
Router> enable
Router# configure terminal
```

b. Configure os nomes de host conforme mostrado na topologia.

```
R1(config)# hostname R1
```

c. Configure endereços IP da interface conforme mostrado na tabela de endereçamento IP.

```
R1(config)# interface g0/0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# no shutdown

R1(config)# interface g0/0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

d. Para evitar que o roteador tente traduzir comandos inseridos incorretamente como se fossem nomes de host, desative a pesquisa de DNS. R1 é mostrado aqui como exemplo.

```
R1(config)#no ip domain-lookup
```

Etapa 3: Configure o roteamento do OSPF nos roteadores.

a. Use o comando **router ospf** no modo de configuração global para ativar o OSPF em R1.

```
R1(config)# router ospf 1
```

b. Configure as instruções **network** para as rede em R1. Use um ID de área igual a 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

c. Configure o OSPF em R2 e R3.

```
R2(config)# router ospf 1
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config)# router ospf 1
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
```

d. Emita o comando **passive-interface** Para alterar a interface G0/0/1 em R1 e R3 para passivo.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0/1

R3(config)# router ospf 1
R3(config-router)# passive-interface g0/0/1
```

Etapa 4: Verifique os vizinhos OSPF e as informações de roteamento.

a. Emita o comando **show ip ospf neighbor** para verificar se cada roteador lista os outros roteadores na rede como vizinhos.

```
R1# show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
10.2.2.2 1 FULL/BDR 00:00:37 10.1.1.2 GigabitEthernet0/0/0
```

b. Emita o comando **show ip route** para verificar se todas as redes são exibidas na tabela de roteamento em todos os roteadores.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set.

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
```

```
C 10.1.1.0/30 is directly connected, GigabitEthernet0/0/0
L 10.1.1.1/32 is directly connected, GigabitEthernet0/0/0
O 10.2.2.0/30 [110/2] via 10.1.1.2, 00:01:11, GigabitEthernet0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
O 192.168.3.0/24 [110/3] via 10.1.1.2, 00:01:07, GigabitEthernet0/0/0
```

Etapa 5: Defina as configurações de IP do host do PC.

Configure um endereço IP estático, máscara de sub-rede e gateway padrão para PC-A e PC-C, conforme mostrado na tabela de endereçamento IP.

Etapa 6: Verifique a conectividade entre PC-A e PC-C.

a. Faça ping de R1 para R3.

   Se os pings não forem bem-sucedidos, identifique e solucione os problemas das configurações básicas dos dispositivos antes de continuar.

b. Ping do PC-A, na LAN R1, para PC-C, na LAN R3.

   Se os pings não forem bem-sucedidos, identifique e solucione os problemas das configurações básicas dos dispositivos antes de continuar.

Nota: Se você puder executar ping do PC-A para o PC-C, você demonstrou que o roteamento OSPF está configurado e funcionando corretamente. Se você não puder fazer ping, mas as interfaces do dispositivo estiverem ativas e os endereços IP estiverem corretos, use os comandos **show run, show ip ospf neighbour** e **show ip route** para ajudar a identificar problemas relacionados ao protocolo de roteamento.

Etapa 7: Salve a configuração básica de execução de cada roteador.

Salve a configuração básica de execução dos roteadores como arquivos de texto em seu PC. Esses arquivos de texto podem ser usados para restaurar as configurações posteriormente no laboratório.

Parte 2: Configure a segurança SNMPv3 usando uma ACL.

O protocolo SNMP (Simple Network Management Protocol) permite que os administradores de rede monitorem o desempenho da rede, gerenciem dispositivos de rede e solucionem problemas de rede. O SNMPv3 fornece acesso seguro autenticando e criptografando pacotes de gerenciamento SNMP na rede. Você configurará o SNMPv3 usando uma ACL em R1.

Etapa 1: Configure uma ACL em R1 que restringirá o acesso ao SNMP na LAN 192.168.1.0.

a. Crie uma lista de acesso padrão chamada **PERMIT-SNMP**.

```
R1(config)# ip access-list standard PERMIT-SNMP
```

b. Adicione uma declaração de permissão para permitir apenas pacotes na LAN de R1.

```
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
```

Etapa 2: Configure a visualização SNMP.

Configure uma visualização SNMP chamada **SNMP-RO** para incluir a família ISO MIB.

```
R1(config)# snmp-server view SNMP-RO iso included
```

Etapa 3: Configure o grupo SNMP.

Chame o nome do grupo **SNMP-G1** e configure o grupo para usar SNMPv3 e exigir autenticação e criptografia usando a palavra-chave **priv**. Associe a visualização que você criou na Etapa 2 ao grupo, dando a ela acesso somente leitura com o parâmetro de leitura **read**. Por fim, especifique o ACL **PERMIT-SNMP**, configurado na Etapa 1, para restringir o acesso SNMP à LAN local.

```
R1(config)# snmp-server group SNMP-G1 v3 priv read SNMP-RO access PERMIT-SNMP
```

Etapa 4: Configure o usuário SNMP.

Configure um usuário **SNMP-Admin** e associe o usuário ao grupo **SNMP-G1** que você configurou na Etapa 3. Defina o método de autenticação como **SHA** e a senha de autenticação como **Authpass**. Use AES-128 para criptografia com uma senha **Encrypass**.

```
R1(config)# snmp-server user SNMP-Admin SNMP-G1 v3 auth sha Authpass priv aes
128 Encrypass
R1(config)# end
```

Etapa 5: Verifique sua configuração SNMP.

a. Use o comando **show snmp group** no modo EXEC de privilégio para visualizar a configuração do grupo SNMP. Verifique se o seu grupo está configurado corretamente.

Nota: Se você precisar fazer alterações no grupo, use o comando **no snmp group** para remover o grupo da configuração e, em seguida, adicione-o novamente com os parâmetros corretos.

```
R1# show snmp group
groupname: ILMI security model:v1
contextname: <no context specified> storage-type: permanent
readview : *ilmi writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI security model:v2c
contextname: <no context specified> storage-type: permanent
readview : *ilmi writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: SNMP-G1 security model:v3 priv
contextname: <no context specified> storage-type: nonvolatile
readview : SNMP-RO writeview: <no writeview specified>
notifyview:
row status: active access-list: PERMIT-SNMP
```

b. Use o comando **show snmp user** para visualizar as informações do usuário SNMP.

Nota: O comando **snmp-server user** está oculto na visualização na configuração por motivos de segurança. No entanto, se você precisar fazer alterações em um usuário SNMP, poderá emitir o comando **no snmp-server user** para remover o usuário da configuração e, em seguida, adicionar novamente o usuário com os novos parâmetros.

```
R1# show snmp user

User name: SNMP-Admin
Engine ID: 800000903007079B3923640
```

```
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: SNMP-G1
```

Parte 3: Configure uma fonte de tempo sincronizada usando NTP.

R2 será a fonte de relógio NTP mestre para os roteadores R1 e R3.

Observação: R2 também pode ser a fonte de relógio mestre para os switches S1 e S3, mas não é necessário configurá-los para este laboratório.

Etapa 1: Configure o NTP Master usando comandos Cisco IOS.

R2 é o servidor NTP mestre neste laboratório. Todos os outros roteadores e switches aprendem o tempo com ele, direta ou indiretamente. Por esse motivo, você deve garantir que R2 tenha o horário universal coordenado correto definido.

a. Use o comando **show clock** para exibir a hora atual definida no roteador.

```
R2# show clock
*18:18:25.443 UTC Sun Jan 31 2021
```

b. Para definir a hora no roteador, use o comando **clock set** *time*.

```
R2# clock set 11:17:00 Jan 31 2021
R2#
*Jan 31 11:17:00.001: %SYS-6-CLOCKUPDATE: System clock has been updated from
18:19:03 UTC Sun Jan 31 2021 to 11:17:00 UTC Sun Jan 31 2021, configured from
console by console.
Jan 31 11:17:00.001: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been
set.
```

c. Configure a autenticação NTP definindo o número da chave de autenticação, o tipo de hashing e a senha que serão usados para autenticação. A senha diferencia maiúsculas de minúsculas.

```
R2# config t
R2(config)# ntp authentication-key 1 md5 NTPpa55
```

d. Configure a chave confiável que será usada para autenticação em R2.

```
R2(config)# ntp trusted-key 1
```

e. Habilite o recurso de autenticação NTP em R2.

```
R2(config)# ntp authenticate
```

f. Configure R2 como o mestre NTP usando o comando **ntp master** *stratum-number* no modo de configuração global. O número do estrato indica a distância da fonte original. Para este laboratório, use um número de estrato **3** em R2. Quando um dispositivo aprende a hora de uma fonte NTP, seu número estrato torna-se um maior que o número estrato de sua fonte.

```
R2(config)# ntp master 3
```

Etapa 2: Configure R1 e R3 como clientes NTP usando o CLI.

a. Emita o comando **debug ntp all** para ver a atividade NTP em R1 à medida que se sincroniza com R2. Revise as mensagens de depuração conforme você prossegue nesta etapa.

```
R1# debug ntp all
NTP events debugging is on
```

```
NTP core messages debugging is on
NTP core messages debugging is on
NTP reference clocks debugging is on
NTP packets debugging is on
```

b. Configure a autenticação NTP definindo o número da chave de autenticação, o tipo de hashing e a senha que serão usados para autenticação.

```
R1#config t
R1(config)# ntp authentication-key 1 md5 NTPpassword
R1(config)#
*Jan 31 18:41:23.707: NTP Core(INFO): keys initilized.
*Jan 31 18:41:23.712: NTP Core(NOTICE): proto: precision = usec
*Jan 31 18:41:23.712: %NTP : Drift Read Failed (String Error).
*Jan 31 18:41:23.712: NTP Core(DEBUG): drift value read: 0.000000000
*Jan 31 18:41:23.712: NTP Core(NOTICE): ntpd PPM
*Jan 31 18:41:23.712: NTP Core(NOTICE): trans state : 1
*Jan 31 18:41:23.712: NTP: Initialized interface GigabitEthernet0/0/0
*Jan 31 18:41:23.712: NTP: Initialized interface GigabitEthernet0/0/1
*Jan 31 18:41:23.712: NTP: Initialized interface LIIN0
R1(config)#
*Jan 31 18:41:23.713: NTP Core(INFO): more memory added for keys.
*Jan 31 18:41:23.713: NTP Core(INFO): key (1) added.
```

c. Configure the trusted key that will be used for authentication. Este comando fornece proteção contra a sincronização acidental do dispositivo com uma fonte de tempo não confiável.

```
R1(config)# ntp trusted-key 1
R1(config)#
*Jan 31 18:43:56.191: NTP Core(INFO): key (1) marked as trusted.
```

d. Ative o recurso de autenticação NTP.

```
R1(config)# ntp authenticate
R1(config)#
*Jan 31 18:44:33.482: NTP Core(INFO): 0.0.0.0 C01C 0C clock_step
```

e. R1 e R3 se tornarão clientes NTP de R2. Use o comando **ntp server** *hostname.* O nome do host também pode ser um endereço IP.

Nota: O comando **ntp update-calendar** pode ser necessário para atualizar periodicamente o calendário com a hora NTP para outras imagens IOS.

```
R1(config)# ntp server 10.1.1.2
R1(config)#
*Jan 31 18:45:29.714: NTP message sent to 10.1.1.2, from interface
'GigabitEthernet0/0/0' (10.2.2.1).
*Jan 31 18:45:29.715: NTP message received from 10.1.1.2 on interface
'GigabitEthernet0/0/0' (10.2.2.1).
*Jan 31 18:45:29.716: NTP Core(DEBUG): ntp_receive: message received
*Jan 31 18:45:29.716: NTP Core(DEBUG): ntp_receive: peer is 0x80007FA135BB32F8, next
action is 1.
*Jan 31 18:45:29.716: NTP Core(DEBUG): Peer becomes reachable, poll set to 6.

*Jan 31 18:45:29.716: NTP Core(INFO): 10.1.1.2 8014 84 reachable
*Jan 31 18:45:29.716: NTP Core(INFO): 10.1.1.2 962A 8A sys_peer
```

```
R1(config)#
*Jan 31 18:45:29.716: NTP: step(0xFFFF9D56.B5A1C9F4): local_offset =
0x00000000.00000000, curtime = 0xE3C17949.B74BC8A0
*Jan 31 11:44:32.426: NTP Core(NOTICE): time reset -25257.290500 s
*Jan 31 11:44:32.426: NTP Core(NOTICE): trans state : 4
*Jan 31 11:44:32.426: NTP Core(INFO): 0.0.0.0 C62C 0C clock_step
*Jan 31 11:44:32.426: NTP Core(INFO): 0.0.0.0 C03C 0C clock_step
*Jan 31 11:44:33.423: NTP message sent to 10.1.1.2, from interface
'GigabitEthernet0/0/0' (10.2.2.1).
*Jan 31 11:44:33.424: NTP message received from 10.1.1.2 on interface
'GigabitEthernet0/0/0' (10.2.2.1).
*Jan 31 11:44:33.424: NTP Core(DEBUG): ntp_receive: message received
*Jan 31 11:44:33.424: NTP Core(DEBUG): ntp_receive: peer is 0x80007FA135BB32F8, next
action is 1.
*Jan 31 11:44:33.424: NTP Core(DEBUG): Peer becomes reachable, poll set to 6.

*Jan 31 11:44:33.424: NTP Core(INFO): 10.1.1.2 8034 84 reachable
*Jan 31 11:44:33.425: NTP Core(INFO): 10.1.1.2 964A 8A sys_peer
```

f. Emita o comando **undebug all** ou **no debug ntp all** para desligar a depuração.

```
R1# undebug all
```

g. Verifique se R1 fez uma associação com R2 com o comando **show ntp associations**. Você também pode usar a versão mais detalhada do comando, adicionando o argumento **detail**. It might take some time for the NTP association to form.

```
R1# show ntp associations

address ref clock st when poll reach delay offset disp
~10.1.1.2 127.127.1.1 3 14 64 3 0.000 -280073 3939.7
*sys.peer, # selected, +candidate, -outlyer, x falseticker, ~ configured
```

h. Verify the time on R1 after it has made an association with R2.

```
R1# show clock
*11:49:27.709 UTC Sun Jan 31 2021
```

i. Repeat the NTP configurations to configure R3 as an NTP client.

Parte 4: Configure o suporte syslog em R1 e PC-A.

Etapa 1: Instale e inicie o servidor syslog.

Versões gratuitas ou de teste do servidor syslog podem ser baixadas da Internet. Use um navegador da web para pesquisar “servidor syslog gratuito do Windows” e consulte a documentação do software para obter mais informações. Seu instrutor também pode recomendar um servidor syslog adequado para uso em sala de aula.

Se um servidor syslog não estiver instalado no host, baixe um servidor syslog e instale-o no PC-A. Se já estiver instalado, vá para a próxima etapa.

Etapa 2: Configure R1 para registrar mensagens no servidor syslog usando o CLI.

a. Inicie o servidor syslog.

b. Verifique que você tem a conectividade entre o R1 e o PC-A fazendo ping o endereço IP 192.168.1.1 da interface R1 G0/0/1. Se não for bem sucedido, pesquise defeitos conforme necessário antes de continuar.

c. O NTP foi configurado em uma parte anterior para sincronizar o tempo na rede. Indicar a hora e a data corretas nas mensagens do syslog é vital ao usar o syslog para monitorar uma rede. Se a hora e a data corretas de uma mensagem não forem conhecidas, pode ser difícil determinar qual evento de rede causou a mensagem.

   Verifique se o serviço de carimbo de data / hora para registro está habilitado no roteador usando o comando **show run**. Use o seguinte comando se o serviço de carimbo de data / hora não estiver habilitado.

```
R1(config)# service timestamps log datetime msec
```

d. Configurar o serviço do syslog no roteador para enviar mensagens de syslog ao servidor de syslog.

```
R1(config)# logging host 192.168.1.3
```

Etapa 3: Configurar o nível de gravidade de registro no R1.

As trap de registro podem ser definidas para suportar a função de registro. Uma trap é um ponto inicial que, quando atingido, aciona uma mensagem de log. O nível de mensagens de registro pode ser ajustado para permitir que o administrador determine que tipos das mensagens são enviadas ao servidor do syslog. Os roteadores suportam diferentes níveis de registro. Os oito níveis variam de 0 (emergências), indicando que o sistema é instável, a 7 (depuração), que envia mensagens que incluem informações de roteador.

Nota: O nível padrão para o syslog é 6, registro informativo. O padrão para o registro do console e do monitor é 7, depuração.

a. Use o comando **logging trap** para determinar as opções do comando e os vários níveis de trap disponíveis.

```
R1(config)# logging trap ?
<0-7> Logging severity level
alerts Immediate action needed (severity=1)
critical Critical conditions (severity=2)
debugging Debugging messages (severity=7)
emergencies System is unusable (severity=0)
errors Error conditions (severity=3)
informational Informational messages (severity=6)
notifications Normal but significant conditions (severity=5)
warnings Warning conditions (severity=4)
<cr>
```

b. Defina o nível de gravidade para as mensagens enviadas ao servidor do syslog. Para configurar os níveis de gravidade, use a palavra-chave ou o número do nível de gravidade (0—7).

Nível de gravidade	Palavra-chave	Significado
0	emergencies	O sistema não pode ser usado
1	alerts	Ação imediata necessária
2	critical	Condições críticas
3	errors	Condições de erro
4	warnings	Condições de advertência
5	notifications	Condição normal, mas significativa
6	informational	Mensagens informativas

7	debugging	Mensagens de depuração

Nota: O nível de gravidade inclui o nível especificado e qualquer coisa com um número de gravidade mais baixo. Por exemplo, se você definir o nível como 4, ou usar os **avisos de palavra-chave**, você captura mensagens com nível de gravidade 4, 3, 2, 1 e 0.

c. Use o comando **logging trap** ajustar o nível de gravidade para R1.

```
R1(config)# logging trap warnings
```

Qual é o problema em definir o nível de gravidade muito alto ou muito baixo?

Se o comando **logging trap warnings** tiver sido emitido, quais níveis de gravidade de mensagens serão registrados?

Etapa 4: Exiba o status atual do registro para R1.

a. Use o comando **show logging** ver o tipo e o nível de registro permitidos.

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 72 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level debugging, 72 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level warnings, 54 message lines logged
        Logging to 192.168.1.3 (udp port 514, audit disabled,
              link up),
              3 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
```

```
               filtering disabled
        Logging Source-Interface: VRF Name:
<output omitted>
```

Em que nível o log do console está habilitado?

O trap logging está ativado em qual nível?

Qual é o endereço IP do Servidor syslog?

Qual porta o syslog está usando?

Etapa 5: Faça alterações ao roteador e monitore os resultados do syslog no PC.

a. Verifique que o servidor de syslog já está iniciado no PC-A. Inicie o servidor conforme necessário.

b. Para verificar que o servidor do syslog está registrando a mensagem, desabilite e permita a relação G0/0/0 do R1.

```
R1(config)# interface g0/0/0
R1(config-if)# shut
.Jan 31 12:02:50.376: %LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state
to administratively down
.Jan 31 12:02:51.376: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to down
R1(config-if)# no shut
.Jan 31 12:03:11.302: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.4 port
514 started - CLI initiated
.Jan 31 12:03:14.365: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to
up
.Jan 31 12:03:15.365: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to up
.Jan 31 12:03:59.894: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on GigabitEthernet0/0/0
from LOADING to FULL, Loading Done
```

c. Navegue ao PC-A para ver as mensagens do syslog.

Tabela de resumo das interfaces dos roteadores

Modelo do roteador	Interface Ethernet 1	Interface Ethernet 2	Interface serial 1	Interface serial 2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Modelo do roteador	Interface Ethernet 1	Interface Ethernet 2	Interface serial 1	Interface serial 2
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Nota: Para descobrir como o roteador está configurado, consulte as interfaces para identificar o tipo de roteador e quantas interfaces o roteador possui. Não há como listar efetivamente todas as combinações de configurações para cada classe de roteador. Esta tabela inclui identificadores para as combinações possíveis de Ethernet e Interfaces seriais no dispositivo. Esse tabela não inclui nenhum outro tipo de interface, embora um roteador específico possa conter algum. Um exemplo disso poderia ser uma interface ISDN BRI. A string entre parênteses é a abreviatura legal que pode ser usada no comando do Cisco IOS para representar a interface.