Guia dos Usuários do
IBM gSecurity QRadar
Versão 7.2.5

Packet Capture

Nota

Antes de usar estas informações e o produto que elas suportam, leia as informações em “Avisos” na página 19.

Informações do produto

Esse documento se aplica ao IBM QRadar Security Intelligence Platform V7.2.5 e às liberações subsequentes a menos que seja substituído por uma versão atualizada desse documento.

Índice

Sobre este guia do usuário do Packet Capture

Esta documentação fornece a você as informações necessárias para instalar e configurar o IBM® Security QRadar Packet Capture. O QRadar Packet Capture é suportado pelo IBM Security QRadar SIEM.

Público desejado

Os administradores de sistemas que são responsáveis por instalar o QRadar Packet Capture devem estar familiarizados com os conceitos de segurança de rede e as configurações de dispositivo.

Documentação técnica

Para localizar a documentação do produto IBM Security QRadar na biblioteca de produtos QRadar, consulte Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Entrando em contato com o suporte ao cliente

Para obter informações sobre como entrar em contato com o suporte ao cliente, consulte a Nota técnica de suporte e download (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Declaração de boas práticas de segurança

A segurança do sistema de TI envolve a proteção de sistemas e informações por meio da prevenção, detecção e resposta ao acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar em informações que são alteradas, destruídas, desapropriadas ou usadas indevidamente ou pode resultar em dano ou uso indevido dos sistemas, inclusive para uso em ataques a outros. Nenhum sistema ou produto de TI deve ser considerado completamente seguro e nenhum único produto, serviço ou medida de segurança pode ser completamente efetivo na prevenção de uso ou acesso incorreto. Os sistemas, produtos e serviços IBM são projetados para fazerem parte de uma abordagem de segurança legal abrangente, que envolverá necessariamente procedimentos operacionais adicionais e poderá requerer que outros sistemas, produtos ou serviços sejam mais efetivos. A IBM NÃO GARANTE QUE QUAISQUER SISTEMAS, PRODUTOS OU SERVIÇOS SÃO IMUNES, OU DEIXARÃO SUA EMPRESA IMUNE, DE CONDUTAS ILEGAIS OU MALICIOSAS DE QUALQUER PARTE.

Observe que:

O uso desse programa pode implicar em várias leis ou regulamentos. incluindo aqueles relacionados à privacidade, proteção de dados, empregabilidade, e comunicações e armazenamento eletrônicos. O IBM Security QRadar pode ser usado somente para propósitos legais e de uma forma legal. O cliente concorda em usar este programa conforme as leis aplicáveis, regulamentos e políticas e assume todas as responsabilidades para obedecê-las. O licenciado declara que obterá ou obteve consentimentos, permissões ou licenças necessários para possibilitar seu uso legal do IBM Security QRadar.

Capítulo 1. O que há de novo para usuários do QRadar Packet Capture V7.2.5

O IBM Security QRadar Incident Forensics V7.2.5 apresenta novas instalações de dispositivo, novo hardware e novo software do QRadar Packet Capture Data Node.

Dispositivos do QRadar Packet Capture Data Node para mais armazenamento

Para mais capacidade de armazenamento, é possível conectar no máximo dois dispositivos do QRadar Packet Capture Data Node a um dispositivo da captura de pacote principal. Cada dispositivo do QRadar Packet Capture Data Node fornece 30 TB extras de armazenamento. QRadar Packet Capture Data Nodes são suportados somente nos dispositivos IBM System x3650 M4.

Para obter mais informações, consulte o *IBM Security QRadar Packet Capture Quick Reference Guide*.

Nós principais do QRadar Packet Capture disponíveis em dispositivos Dell

Os nós principais do QRadar Packet Capture estão disponíveis nos dispositivos Dell R730. A configuração de clusters com QRadar Packet Capture Data Nodes não é suportada nos dispositivos Dell.

Para obter mais informações, consulte *IBM Security QRadar Packet Capture Quick Reference Guide*.

Procurar captura de pacote de rede por um período de tempo especificado para propósitos de diagnóstico

O dado do índice criado no tempo de captura é usado para produzir um arquivo de captura de pacote (pcap) que contém informações de pacotes e de metadados de pacotes por um período de tempo especificado. A limpeza manual é necessária, para que a partição de extração não seja preenchida. Saiba mais...

Instalações de software em seu próprio hardware

É possível instalar o QRadar Packet Capture em seu próprio dispositivo. As instalações em dispositivos virtuais não são suportadas.

Para obter mais informações, consulte o *IBM Security QRadar Incident Forensics Installation Guide*.

Dispositivo do QRadar Packet Capture disponível como uma matriz do RAID 5

Para assegurar que os dados sejam protegidos e que possam ser acessados sem interrupção quando houver uma falha do disco online, a partição de armazenamento agora é RAID 5. A partição do sistema operacional é RAID 0.

Capítulo 2. Introdução ao QRadar Packet Capture

IBM Security QRadar Packet Capture é um aplicativo de captura e procura de tráfego de rede.

Com o QRadar Packet Capture, é possível capturar pacotes de rede em taxas de até 10 Gigabit/s a partir de uma interface de rede em tempo real, e gravá-los nos arquivos sem perda de pacote. O QRadar Packet Capture usa o formato de arquivo PCAP padrão para armazenar o tráfego de rede. O formato de arquivo PCAP permite integração fácil com ferramentas existentes de análise de terceiro.

É possível usar o QRadar Packet Capture para procurar o tráfego de rede capturado pelo tempo e os dados de envelope de pacote. Com os recursos de dispositivos e procuras customizadas suficientes, é possível usar dados de procura e de gravador simultaneamente sem perda de dados.

Os arquivos de captura são armazenados em diretórios. Quando o espaço no diretório ficar cheio, os arquivos de captura serão sobrescritos com base nos parâmetros de gravação pré-configurados.

O QRadar Packet Capture pode procurar tráfego de rede capturado por tempo e dados de envelope de pacote. Use a procura simultaneamente com o gravador sem perda de dados, se as procuras estiverem customizadas e os recursos de dispositivo apropriados tiverem sido fornecidos. Ele também fornece gravação de pacote em disco de alto desempenho.

Recursos do QRadar Packet Capture

Alguns recursos inclusos com o QRadar Packet Capture:

Formato de arquivo PCAP padrão

Um formato de arquivo que é usado para armazenar tráfego de rede. O formato de arquivo é integrado às ferramentas de análise de terceiros existentes.

Gravação do pacote para o disco de alto desempenho

Capturar pacotes de rede de uma rede ativa.

Suporte de diversos núcleos

O QRadar Packet Capture está projetado para ser usado com arquitetura de múltiplos núcleos.

Acesso de disco de E/S direta

O QRadar Packet Capture usa o acesso de E/S direta a discos para obter rendimento máximo de gravação de disco.

Indexação em tempo real

O QRadar Packet Capture pode produzir um índice automaticamente durante a captura de pacote. O índice pode ser consultado com sintaxe semelhante ao BPF para recuperar rapidamente pacotes interessantes em um intervalo de tempo especificado.

Capacidade do cluster para aumentar a capacidade de dados de captura.

É possível ativar os nós de dados para criar um cluster para capacidade de armazenamento incluída.

Formato de dump

Os arquivos de captura são salvos no formato PCAP padrão com registros de data e hora em resolução de microssegundo. Arquivos de captura são armazenados em ordem sequencial com base no tamanho do arquivo. Os arquivos de captura são armazenados em diretórios. Quando o espaço no diretório ficar cheio, os arquivos de captura serão sobrescritos com base nos parâmetros de gravação pré-configurados.

Conceitos relacionados:

Capítulo 4, “Visão geral de uso de captura”, na página 9
Para capturar tráfego em disco, inicie o aplicativo de captura. O componente Recorder salva os dados de tráfego em um diretório pré-configurado. Quando o espaço no diretório ficar cheio, os arquivos existentes serão sobrescritos.

Capítulo 3. Configuração do QRadar Packet Capture

Uma configuração inicial básica é necessária antes de usar o IBM Security QRadar Packet Capture.

Navegadores da web suportados

Os navegadores da web a seguir são suportados:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer V10 e posterior

Configurando sua rede

Para tornar o QRadar Packet Capture disponível remotamente, um endereço IP deve ser designado a uma das portas Ethernet, geralmente eth2, eth3 ou eth4. Por padrão, o sistema é configurado para usar DHCP. No entanto, para a configuração inicial, talvez seja necessário conectar um monitor compatível com VGA, iniciar o sistema localmente, efetuar login e configurar um endereço IP estático para sua própria rede. Após iniciar o sistema, efetue login como o usuário raiz usando estas credenciais:

```
username: root
password: P@ck3t08..)
```

Para a configuração inicial, execute estas etapas:

1. Conecte um monitor compatível com VGA.
2. Ligue o dispositivo QRadar Packet Capture.
3. Efetue logon no sistema operacional Linux como usuário raiz.

   `Username: root`

   `Password: P@ck3t08..`

   Para alterar a senha padrão, consulte "Alterando a senha da conta de sistema operacional" na página 6.
4. Para certificar-se de que seu sistema está atualizado, aplique as correções de software disponíveis no IBM Fix Central (www.ibm.com/support/fixcentral/).
5. Configure um endereço IP estático para sua própria rede.
   a. Para obter o endereço MAC ou a interface eth2, digite o seguinte comando:

      `ifconfig | grep eth2`

      As interfaces eth0 e eth1 não estão disponíveis. Use eth2 para o hardware M4 xSeries.
   b. Anote o endereço MAC.
   c. Edite as configurações no arquivo `/etc/sysconfig/network-scripts/ifcfg-eth2`:
      - Inclua o texto a seguir como a primeira linha: `DEVICE=eth2`
      - Remova o comentário do endereço MAC da porta eth2: `HWADDR=xx:xx:xx:xx:xx`
      - Assegure-se de que a configuração a seguir esteja configurada: `BOOTPROTO=static`

- Assegure-se de usar informações que sejam relevantes para sua rede e que a saída seja semelhante ao seguinte exemplo estático:

```
DEVICE=eth2
#HWADDR=xx:xx:xx:xx:xx
BOOTPROTO="static"
BROADCAST="192.168.1.255"
DNS1="0.0.0.0"
DNS2="0.0.0.0"
GATEWAY="192.168.1.2"
IPADDR="192.168.1.1"
NETMASK="255.255.255.0"
NM_CONTROLLED="no"
ONBOOT="yes"
```

6. Salve o arquivo.
7. Para aplicar as configurações, execute o seguinte comando:

   ```
   service network restart
   ```

8. Verifique sua configuração de interface executando o seguinte comando:

   ```
   ifconfig | more
   ```

Exemplo de DHCP: No CentOS6.2, edite as configurações a seguir no arquivo `/etc/sysconfig/network-scripts/ifcfg-eth0` ou `/etc/sysconfig/network-scripts/ifcfg-eth1`.

```
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
```

Login remoto

Após configurar um endereço IP localmente, será possível administrar o dispositivo efetuando login remotamente usando SSH na porta 4477.

Alterando a senha da conta de sistema operacional

Após configurar o dispositivo, altere a senha do sistema operacional padrão para IBM Security QRadar Packet Capture.

Você deve ser o usuário raiz para alterar a conta de sistema operacional.

As senhas do QRadar Packet Capture são independentes das senhas do sistema operacional. As contas do usuário `adminusername` e `continuum` devem alterar suas senhas quando efetuarem login pela primeira vez

Procedimento

1. Use SSH para efetuar login como o usuário-raiz.

   A senha padrão do usuário raiz é `P@ck3t08..`

2. Para alterar as senhas das contas de usuário `continuum` e `root`, use o comando **passwd** *username*.

Sincronizando o tempo de espera do servidor do QRadar Packet Capture com o tempo do sistema do QRadar Console

Para assegurar que as implementações do IBM Security QRadar tenham configurações de tempo consistentes para que as procuras e as funções relacionadas a dados funcionem adequadamente, todos os dispositivos devem sincronizar-se com o dispositivo QRadar Console. Um administrador deve atualizar iptables no dispositivo QRadar Console e configurá-lo para aceitar a comunicação rdate na porta 37.

Antes de Iniciar

Deve-se saber o endereço IP ou nome do host do QRadar Console. O nome do host deve ser resolvido corretamente usando nslookup.

Por padrão, o fuso horário para o dispositivo QRadar Packet Capture está configurado para UTC (Hora Universal Coordenada).

Procedimento

1. Use o SSH para efetuar login no dispositivo QRadar Packet Capture como o usuário raiz.
2. Para desligar o serviço Network Time Protocol (NTP), digite o comando a seguir: `service ntpd stop`.
3. Para desligar a configuração para o NTP, digite o comando a seguir: `chkconfig ntpd off`.
4. Planeje a sincronização como uma tarefa cron editando o arquivo `crontab` (crontable).
   a. Digite o comando a seguir: `crontab -e`.
   b. Para configurar o dispositivo para sincronizar com o QRadar Console a cada 10 minutos, digite o comando a seguir: `*/10 * * * * rdate -s` *`Console_IP_Address`*`.`

      Use um endereço IP ou nome do host para a variável *Console_IP_Address*.
   c. Salve suas mudanças na configuração.
   d. Ative o crond digitando os comandos a seguir:

      ```
      service crond start
      chkconfig crond on
      ```
5. Atualize as iptables no QRadar Console para aceitar o tráfego rdate de dispositivos IBM Security QRadar Packet Capture.
   a. Use o SSH para efetuar login no dispositivo QRadar Console como o usuário raiz.
   b. Edite o arquivo `/opt/qradar/conf/iptables.pre`.
   c. Digite o comando a seguir:

      ```
      -A QChain -m tcp -p tcp --dport 37 -j ACCEPT --src <PCAP_IP address>
      ```

      Se você tiver diversos dispositivos QRadar Packet Capture, inclua cada endereço IP como uma única linha.

      Exemplo:

      ```
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.10
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.11
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.12
      ```
   d. Salve o arquivo `iptables.pre`.

e. Atualize as iptables no QRadar Console digitando o comando a seguir:
   `./opt/qradar/bin/iptables_update.pl`

Conceitos relacionados:

Capítulo 4, “Visão geral de uso de captura”, na página 9
Para capturar tráfego em disco, inicie o aplicativo de captura. O componente Recorder salva os dados de tráfego em um diretório pré-configurado. Quando o espaço no diretório ficar cheio, os arquivos existentes serão sobrescritos.

Capítulo 4. Visão geral de uso de captura

Para capturar tráfego em disco, inicie o aplicativo de captura. O componente Recorder salva os dados de tráfego em um diretório pré-configurado. Quando o espaço no diretório ficar cheio, os arquivos existentes serão sobrescritos.

Resolução de problemas: Se você observar que nenhum dado está sendo coletado, assegure-se de que haja tráfego pelas conexões. Para capturar o tráfego, deve-se usar uma porta Tap ou SPAN (espelho). Ao usar uma porta SPAN em um comutador, se o comutador designar uma prioridade inferior à porta SPAN, alguns pacotes poderão ser eliminados.

Introdução

Após configurar o sistema, efetue login no IBM Security QRadar Packet Capture seguindo estas etapas:

1. Abra um navegador da web e insira o endereço IP do dispositivo.
2. Efetue login usando as seguintes informações sobre o usuário:

   Usuário: `continuum`

   Senha: `P@ck3t08..`

Por padrão, a página Capturar estado é exibida. É possível controlar registros clicando em **Iniciar captura** ou **Parar captura**.

Dica: É possível ver o número da versão de produto no canto superior direito da janela.

Capturar estado

As informações a seguir são fornecidas na página Capturar estado:

- **Captura de interface ativada**
- **Status da captura**
- **Horário de início/parada**
- **Duração de captura do sistema**
- **Taxa de rendimento**
- **Pacotes capturados**
- **Bytes capturados**
- **Pacotes descartados**
- **Espaço de armazenamento disponível**

Em uma configuração de cluster, o uso de armazenamento é exibido para cada nó de dados ativado. Se o QRadar Packet Capture Data Node for inatingível por causa de um problema de configuração de rede ou de uma conexão incorreta, em vez das estatísticas de armazenamento, a mensagem a seguir é exibida: `o nó escravo é ativado, mas é inatingível atualmente.`

Caracterização da rede

Visualize o rendimento da rede em formato gráfico.

O rendimento máximo padrão de captura para disco é de 10 GBps.

Histórico da captura

Visualize o histórico das capturas de pacotes que ocorreram ou estão em andamento.

Compactação sequencial

Para suportar investigações forenses, é possível reter conteúdo de pacote bruto por um tempo maior aumentando a capacidade de armazenamento virtual disponível sem incluir discos físicos. Agora é possível usar a nova opção de compactação sequencial para armazenar quantia maiores de dados no dispositivo QRadar Packet Capture.

A quantia de compactação está relacionada à quantia de conteúdo de vídeo compactado na carga útil. Por exemplo, se você tiver 5% de vídeo compactado na carga útil, obterá uma compactação de 13:1. A proporção de compactação:armazenamento é a proporção entre o tamanho descompactado e o tamanho compactado.

Tabela 1. Proporções de compactação sequencial

Porcentagem (%) de carga útil de vídeo compactado	Compactação: proporção de amplificação de armazenamento
0	17:1
5	13:1
10	6:1
20	4:1
40	2.4:1

Conceitos relacionados:

Capítulo 2, “Introdução ao QRadar Packet Capture”, na página 3
IBM Security QRadar Packet Capture é um aplicativo de captura e procura de tráfego de rede.

Tarefas relacionadas:

“Sincronizando o tempo de espera do servidor do QRadar Packet Capture com o tempo do sistema do QRadar Console” na página 7
Para assegurar que as implementações do IBM Security QRadar tenham configurações de tempo consistentes para que as procuras e as funções relacionadas a dados funcionem adequadamente, todos os dispositivos devem sincronizar-se com o dispositivo QRadar Console. Um administrador deve atualizar iptables no dispositivo QRadar Console e configurá-lo para aceitar a comunicação rdate na porta 37.

Capítulo 5. Criando um cluster para capacidade de armazenamento incluída

Após conectar fisicamente o dispositivo principal do QRadar Packet Capture ao QRadar Packet Capture Date Nodes, deve-se ativar o QRadar Packet Capture Data Nodes. A ativação do QRadar Packet Capture Data Nodes cria um cluster para a capacidade de armazenamento incluída.

Para obter informações sobre como conectar os dispositivos, consulte o Guia de Referência Rápida do *QRadar Packet Capture.*

Restrição: Ao desativar um QRadar Packet Capture Date Node, os dados capturados nesse nó ficam inacessíveis para a recuperação forense.

Procedimento

1. Na página Configuração de Cluster, selecione a caixa para cada QRadar Packet Capture Date Node que você conectou ao dispositivo principal do QRadar Packet Capture.
2. Clique em **Salvar**.

Capítulo 6. Procurando pacotes dentro de uma intervalo de tempo para teste de diagnóstico

O dado do índice criado no tempo de captura é usado para produzir um arquivo de captura de pacote (pcap) que contém os pacotes que correspondem ao intervalo de tempo especificado e às informações de metadados do pacote.

Restrição: Essas procuras são somente para propósitos de diagnóstico. A limpeza manual é necessária para evitar o preenchimento da partição de extração.

Procedimento

1. Clique na página **Procurar Pacotes com Linha de Tempo**.

   Os valores padrão já estão inseridos.
2. Selecione a interface para o tráfego capturado que deseja procurar.

   Se você tiver uma única configuração de interface, ela será selecionada automaticamente.
3. Especifique um valor ou altere os padrões para o início e o término do intervalo de tempo no qual deseja procurar.
4. Especifique um Berkeley Packet Filter (BPF).

   Use a sintaxe de BPF para especificar os filtros BPF. Uma expressão consiste em uma ou mais primitivas. As expressões de filtros complexas são construídas usando os operadores AND, OR e NOT.

   Estes exemplos são filtros primitivos

   ```
   ether host 00:11:22:33:44:55
   ether src host 00:11:22:33:44:55

   ip host 192.168.0.1
   ip dst host 192.168.0.1

   ip6 host 2001:0db8:85a3:0042:0000:8a2e:0371:7334
   ip6 src host 2001:0db8:85a3:0042:0000:8a2e:0371:7334

   ip net 192.168.1.0/24
   ip src net 192.168.1

   port 80
   udp port 9000
   tcp src port 80
   ```

   Estes exemplos são filtros complexos

   ```
   ip host 192.168.1.1 and 192.168.1.2
   ip src 192.168.1.1 and dst 192.168.1.2
   ip host 192.168.1.1 and tcp port (80 or 443)
   (ip host 192.168.1.1 or 192.168.1.2) and (port 80 or 443)
   ```
5. Especifique o número de pacotes a serem extraídos.

   O número máximo padrão de pacotes a extrair é 10.000. Se você alterar o número para 0, todos os pacotes que correspondem à linha de tempo e ao filtro serão extraídos.
6. Clique em **Iniciar Procura**.
7. Para ver o estado da fila de procura, clique na página **Fila de Procura**.
8. Para ver o histórico de todas as procuras concluídas, clique nas exibições da página **Procuras Concluídas**.

9. Limpe as procuras manuais para assegurar espaço suficiente para processos de recuperação forense:
   a. Efetue login como raiz.

      nome de usuário: raiz

      senha: P@ck3t08..
   b. Execute o comando a seguir:

      `rm -r /extraction/<name_of_search>`

      A variável *<name_of_search>* é a coluna de nome na página Procuras Concluídas.

Capítulo 7. Solucionando problemas do QRadar Packet Capture

A resolução de problemas é uma abordagem sistemática para solucionar um problema. O objetivo desta resolução de problemas é determinar por que algo não funciona conforme o esperado e explicar como resolver o problema.

A porta de captura está conectada corretamente?

O dispositivo IBM Security QRadar Packet Capture pode ser capturado somente na Interface 0. A imagem a seguir mostra a conexão na parte traseira do sistema, que é a Interface 0:

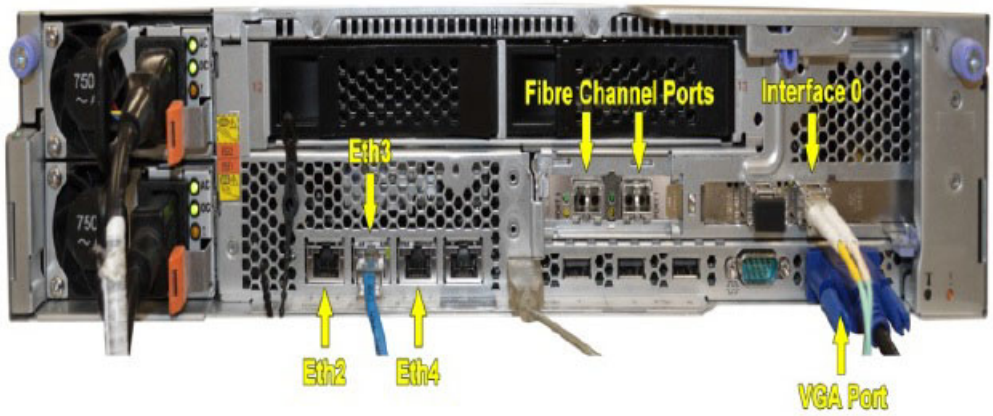

Figura 1. Painel traseiro do QRadar Packet Capture

A conexão de rede Ethernet está configurada corretamente?

Para assegurar que uma interface Ethernet esteja designada a um endereço IP, execute o comando `ifconfig` para a interface que está conectada.

Se nenhum endereço estiver configurado, edite o `ifcfg-eth*` correspondente para configurar um endereço.

- Nesse exemplo de DHCP, edite as configurações a seguir em `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`* e substitua *eth2* pela configuração apropriada.

```
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
```

- Nesse exemplo de endereço IP estático, edite as configurações a seguir em `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`* e substitua *eth2* pela configuração apropriada.

```
BOOTPROTO="static"
BROADCAST="192.168.1.255"
DNS1="0.0.0.0"
DNS2="0.0.0.0"
GATEWAY="192.168.1.2"
IPADDR="192.168.1.1"
NETMASK="255.255.255.0"
NM_CONTROLLED="no"
ONBOOT="yes
```

Após ter alterado as configurações, execute o comando `ifconfig` para configurar a interface de rede.

O tempo do sistema está configurado corretamente?

Por padrão, o tempo do sistema é configurado para a Hora Universal Coordenada (UTC) e é configurado para usar o Network Time Protocol (NTP) e os servidores públicos a fim de manter o tempo do sistema correto.

Há problemas de hardware do sistema?

1. Assegure-se de que o tráfego esteja sendo gerado adequadamente e esteja sendo recebido pela Placa da Interface de Rede (NIC).

   Verifique as luzes imediatamente à direita da conexão da Interface 0. A inferior deve estar ligada continuamente, o que significa uma ligação. A superior deve estar piscando, o que significa uma atividade de tráfego.
2. Execute o comando `/usr/local/nc/bin/dpdk_nic_bind.py –status`.

   O resultado do comando deve ser parecido com a saída a seguir:

```
Network devices using DPDK-compatible driver
============================================
0000:0f:00.0 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
0000:0f:00.1 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
Network devices using kernel driver
===================================
0000:07:00.0 'I350 Gigabit Network Connection' if=eth2 drv=igb unused=igb_uio
*Active*
0000:07:00.1 'I350 Gigabit Network Connection' if=eth3 drv=igb unused=igb_uio
0000:07:00.2 'I350 Gigabit Network Connection' if=eth4 drv=igb unused=igb_uio
Other network devices
=====================
<none>
```

O sistema está capturando tráfego?

Para confirmar se o sistema está capturando tráfego após o início de uma sessão de captura, use um dos métodos a seguir:

- Verifique as luzes imediatamente à direita da conexão da Interface 0. A superior deve estar piscando, o que significa uma atividade de tráfego.
- Na página Caracterização da rede, você verá um resultado gráfico.
- Na linha de comandos, execute o comando `du –h /storage0/int0`.

  O resultado se parece com a saída a seguir:

```
4.4G /storage0/int0/1_0
4.9G /storage0/int0/2_0
6.4G /storage0/int0/3_0
4.9G /storage0/int0/4_0
4.9G /storage0/int0/5_0
4.9G /storage0/int0/6_0
.
.
.
1.4T /storage0/int0/
```

  Se você executar esse comando repetidamente, o número de subdiretórios e as quantias de alocação retornados aumentarão.

A interface REST está funcionado?

Execute o comando a seguir e substitua a senha pela senha correta (não padrão) para o usuário continuum:

```
curl -k -v -X POST -G -d "username=continuum&password=password&action
=ping" https://localhost/rest/forensics_fetch.php
```

O resultado se parece com a saída a seguir:

```
About to connect() to localhost port 443 (#0)
* Trying ::1... connected
* Connected to localhost (::1) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* warning: ignoring value of ssl.verifyhost
* skipping SSL peer certificate verification
* SSL connection using TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* Server certificate:
* subject: E=root@localhost.localdomain,CN=localhost.localdomain,
OU=SomeOrganizationalUnit,
O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
* start date: Mar 27 17:10:01 2014 GMT
* expire date: Mar 27 17:10:01 2015 GMT
* common name: localhost.localdomain
* issuer: E=root@localhost.localdomain,CN=localhost.localdomain,
OU=SomeOrganizationalUnit,
O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
> POST /rest/forensics_fetch.php?username=continuum&password=
test&action=ping HTTP/1.1
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.15.3
zlib/1.2.3 libidn/1.18 libssh2/1.4.2
> Host: localhost
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Mon, 13 Oct 2014 20:08:20 GMT
< Server: Apache/2.2.15 (Red Hat)
< X-Powered-By: PHP/5.3.3
< Set-Cookie: PHPSESSID=54cf36otmg899b6bau03lu6jh6; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Content-Length: 85
< Connection: close
< Content-Type: application/json
<
* Closing connection #0
{"status":"success","message":"QRadar Packet Capture (c), Version 7.2.4.209\n"}
```

Como reconfigurar a senha de usuário continuum

Não é possível alterar a senha de usuário continuum na interface com o usuário do QRadar Packet Capture. Para reconfigurar a senha para o padrão de fábrica, deve-se usar o script `reset_default.sh`. É solicitado que o usuário altere a senha no próximo login.

Para executar o script `reset_default.sh`, efetue login na linha de comandos como usuário raiz e digite o comando a seguir:

```
sh /var/www/html/mysql/reset_default.sh continuum
```

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local:

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Os licenciados deste programa que desejarem obter informações sobre este assunto com o propósito de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações trocadas, deverão entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

Os preços da IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso prévio. Os preços do revendedor podem variar.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos incluem nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com os nomes e endereços utilizados por uma empresa real é mera coincidência.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

Marcas comerciais

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos de marca comercial da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca comercial (® ou ™), estes símbolos indicarão marcas comerciais dos Estados Unidos ou de direito consuetudinário de propriedade da IBM no momento em que estas informações foram publicadas. Estas marcas comerciais também podem ser marcas registradas ou de direito consuetudinário em outros países. Uma lista atual de marcas comerciais da IBM está disponível na web em Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou marcas de serviço de terceiros.

Considerações de política de privacidade

Produtos IBM Software, incluindo soluções de software como serviço, (“Ofertas de Software”) podem usar cookies ou outras tecnologias para coletar informações de uso do produto, para ajudar a melhorar a experiência do usuário final, customizar interações com o usuário final ou para outros propósitos. Em muitas casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar a permitir que você colete informações pessoalmente identificáveis. Se esta Oferta de Software usar cookies para coletar informações pessoalmente identificáveis, informações específicas sobre este uso de oferta de cookies desta oferta serão apresentadas a seguir.

Dependendo das configurações implementadas, esta Oferta de Software pode usar cookies de sessão que coletam o ID de sessão de cada usuário para propósitos de gerenciamento de sessões e autenticação. Esses cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade ativada por eles.

Se as configurações implementadas para esta Oferta de Software fornecerem a você, como cliente, a capacidade de coletar informações pessoalmente identificáveis dos usuários finais por meio de cookies e outras tecnologias, deve-se buscar o seu próprio conselho jurídico a respeito de quaisquer leis aplicáveis a tal coleta de dados, incluindo quaisquer requisitos de aviso e consentimento.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, consulte a Política de Privacidade da IBM em http://www.ibm.com/privacy e a Declaração de Privacidade Online da IBM na seção http://www.ibm.com/privacy/details titulada “Cookies, web beacons e outras tecnologias” e a “Declaração de privacidade de software como serviço e de produtos de software IBM” em http://www.ibm.com/software/info/product-privacy.