IBM Security QRadar Incident Forensics
Versão 7.3.0

QRadar Packet Capture Guia dos Usuários

Nota

Antes de usar estas informações e o produto que ela suporta, leia as informações em “Avisos” na página 27.

Informações do produto

Esse documento se aplica ao IBM QRadar Security Intelligence Platform V7.3.0 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.

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 Acessando a nota técnica da documentação do IBM Security (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 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 as informações através da prevenção, detecção e resposta para acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar em alteração, destruição, desapropriação ou mal uso de informações ou pode resultar em danos ou mau uso dos sistemas, incluindo seu uso em ataques a outros sistemas. Nenhum produto ou sistema de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança individual pode ser completamente eficaz na prevenção do acesso ou uso impróprio. AIBM sistemas, produtos e serviços são projetados para fazerem parte de uma abordagem de segurança abrangente legal, que envolverá necessariamente procedimentos operacionais adicionais, podendo requerer outros sistemas, produtos ou serviços para que sejam mais eficientes. A IBM NÃO GARANTE QUE OS SISTEMAS, PRODUTOS OU SERVIÇOS ESTEJAM IMUNES OU TORNAM A SUA EMPRESA IMUNE CONTRA CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PESSOA.

Observe que:

O uso desse programa pode implicar em várias leis ou regulamentações, incluindo aquelas relacionadas à privacidade, proteção de dados, emprego, e armazenamento e comunicações eletrônicas. O IBM Security QRadar pode ser usado apenas para propósitos legais e de maneira legal. O cliente concorda em usar este Programa de acordo com leis, regulamentos e políticas e assume toda a responsabilidade pelo seu cumprimento. O licenciado declara que obterá ou obteve quaisquer consentimentos, permissões ou licenças necessárias para permitir o uso legal do IBM Security QRadar.

Capítulo 1. Introdução ao QRadar Packet Capture

IBM Security QRadar Packet Capture é um aplicativo de captura e procura de tráfego de rede. O dispositivo QRadar Packet Capture possui somente uma porta de captura (DNA0) e é possível instalar um transceptor SFP de 10G ou 1G.

Com o QRadar Packet Capture, é possível capturar pacotes de rede em taxas de até 10 Gbps a partir de uma interface de rede em tempo real e gravá-los nos arquivos sem perda de pacote.

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

Dispositivos QRadar Packet Capture que possuem um transceptor 10G suportam clusters que expandem a capacidade geral de armazenamento de dados e computacional em comparação a um único servidor independente. Dispositivos QRadar Packet Capture que possuem um transceptor 1G não suportam clusters.

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 a partir de uma rede em tempo real.

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 Berkeley Packet Filter (BPF) e/ou domínio HTTP (Protocolo de Transporte de Hipertexto) ou sequências URL (Localizador Uniforme de Recursos) para recuperar rapidamente pacotes interessantes em um intervalo de tempo especificado.

Capacidade do cluster para aumentar a capacidade de dados de captura (somente edição 10G).

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.

Velocidade da captura

Para dispositivos de captura de pacote, a velocidade de captura do tráfego de rede depende de você ter nós de dados conectado ao nó principal:

- Para dispositivos de captura de pacote que não possuem nós de dados conectados, a velocidade máxima da captura é de até 7 Gbps.
- Para dispositivos de captura de pacote que possuem nós de dados conectados ao nó principal, a velocidade da captura aumenta até 10 Gbps.

Para obter mais informações sobre encaminhamento de pacotes para o QRadar Packet Capture, consulte o *Guia de Administração do IBM Security QRadar*.

Conceitos relacionados:

Capítulo 3, “Visão geral de uso de captura”, na página 7
Para capturar tráfego em disco, inicie o aplicativo de captura. O componente Recorder salva os dados de tráfego de rede em um diretório pré-configurado. Quando o espaço no diretório ficar cheio, os arquivos existentes serão sobrescritos.

Capítulo 2. Configuração do QRadar Packet Capture

É necessária alguma configuração básica antes de usar o IBM Security QRadar Packet Capture.

Navegadores da web suportados

Os navegadores da web a seguir são suportados:

- Google Chrome Versão 44.0.2403.157 ou mais recente.
- Mozilla Firefox Versão 40.0.3 ou mais recente.

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. Para a configuração inicial, talvez seja necessário conectar um monitor compatível com VGA.

Para a configuração inicial, execute as etapas a seguir:

1. Ligue o dispositivo QRadar Packet Capture.
2. Use SSH e a porta 4477 para efetuar login como o usuário raiz.

   O nome de usuário padrão é: `raiz`. A senha padrão é: `P@ck3t08..`

   Para alterar a senha padrão, consulte "Alterando a senha da conta de sistema operacional" na página 5.
3. Para certificar-se de que seu sistema está atualizado, aplique as correções de software disponíveis no IBM Fix Central (www.ibm.com/support/fixcentral/).
4. 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"
        ```
5. Salve o arquivo.
6. Para aplicar as configurações, execute o seguinte comando:

```
service network restart
```

7. 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.

Configurando sua licença

Antes de usar o QRadar Packet Capture, deve-se configurar uma licença para o dispositivo QRadar Packet Capture e para o software QRadar Packet Capture.

Procedimento

1. Para configurar o licenciamento para um dispositivo QRadar Packet Capture que tem um transceptor SFP 1G instalado, conclua as etapas a seguir:
   a. Entre em contato com seu representante IBM para obter a chave de licença para o nó principal.
   b. No QRadar Packet Capture, clique em **Ajuda** > **Atualizar licença principal**.
   c. Para aplicar uma licença a um dispositivo QRadar Packet Capture, cole o valor no campo **Chave de licença**.
   d. Cole os valores para o **ID do sistema** e a **Chave de licença** em seus respectivos campos.
   e. Clique em **Atualizar licença principal** para aplicar as mudanças.
2. Para configurar o licenciamento para um dispositivo QRadar Packet Capture que tem um transceptor SFP+ 10G instalado, conclua as etapas a seguir:
   a. Entre em contato com seu representante IBM para obter uma chave de licença para seus nós de dados.
   b. No QRadar Packet Capture, para aplicar a licença principal, clique em **Ajuda** > **Atualizar licença principal**.
   c. Cole os valores para **Chave de licença** e **ID do sistema** em seus respectivos campos.
   d. Clique em **Atualizar licença principal** para aplicar as mudanças.
   e. Dependendo do número de nós de dados que você tem em um cluster, será necessário atualizar clicando em **Ajuda** > **Node1**.
   f. Para atualizar as licenças dos nós de dados, cole os valores para **Chave de licença** e **ID do sistema** em seus respectivos campos.
   g. Para atualizar o nó de dados, clique em **Atualizar licença do Node1** para aplicar as mudanças.

Administrando usuários

Para permitir que usuários acessem e usem o IBM Security QRadar Packet Capture, deve-se incluir um usuário, designá-lo a uma função apropriada e configurar suas credenciais de login.

Antes de Iniciar

Certifique-se de estar com login efetuado no QRadar Packet Capture como o usuário `raiz`. Ou, como alternativa, assegure-se de que é possível usar um comando `sudo` para criar um usuário.

Procedimento

1. Para criar um usuário, execute o comando a seguir:

   ```
   ./usr/local/nc/bin/nc_user_manager add <username> <password>
   <Admin|Guest>
   ```

   Se já houver um nome do usuário existente <*username*>, esse comando falhará.

   Se a função especificada não for nem administrador, nem convidado, esse comando falhará.

   Quando um usuário for incluído, será possível usar o mesmo nome do usuário e senha para o login do produto e para o login da API REST.
2. Para excluir um usuário, execute o comando a seguir:

   ```
   ./usr/local/nc/bin/nc_user_manager delete <username> <password>
   ```

   Se já houver um nome do usuário existente <*username*>, esse comando falhará.

   Esse comando falhará se <*username*> e <*password*> não corresponderem ao que está registrado no QRadar Packet Capture.

   Quando um usuário for excluído, será possível usar o mesmo nome do usuário e senha para o login do produto e para o login da API REST.

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 aplicativo QRadar Packet Capture são independentes das senhas do sistema operacional.

Procedimento

1. Use o SSH para efetuar login como o usuário `root`.

   A senha padrão do usuário raiz é `P@ck3t08..`
2. Para mudar a senha das contas de usuário `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 `root`.
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 QRadar Packet Capture.
   a. Use o SSH para efetuar login no dispositivo QRadar Console como o usuário `root`.
   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:

```
-A QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.10
-A QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.11
-A 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 3, “Visão geral de uso de captura”, na página 7
Para capturar tráfego em disco, inicie o aplicativo de captura. O componente Recorder salva os dados de tráfego de rede em um diretório pré-configurado. Quando o espaço no diretório ficar cheio, os arquivos existentes serão sobrescritos.

Capítulo 3. Visão geral de uso de captura

Para capturar tráfego em disco, inicie o aplicativo de captura. O componente Recorder salva os dados de tráfego de rede 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 digite a URL a seguir:
   `https://PCAP_IP_Address:41390`
2. Efetue login usando as informações de contas dos usuários a seguir:
   Usuário: `continuum`
   Password: `P@ck3t08..`

Resolução de problemas: Se um usuário falhar em fornecer a senha correta cinco vezes consecutivas em um período de 10 minutos, o usuário será bloqueado durante 30 minutos. A conta do usuário pode ser desbloqueada manualmente por um administrador do sistema.

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

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.`

Resolução de problemas

Para visualizar as informações do sistema sobre as interfaces de captura configuradas, clique em **Resolução de problemas**.

Informações do servidor

Para visualizar as informações de armazenamento do servidor, clique em **Informações do servidor**.

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 1, “Introdução ao QRadar Packet Capture”, na página 1
IBM Security QRadar Packet Capture é um aplicativo de captura e procura de tráfego de rede. O dispositivo QRadar Packet Capture possui somente uma porta de captura (DNA0) e é possível instalar um transceptor SFP de 10G ou 1G.

Tarefas relacionadas:

"Sincronizando o tempo de espera do servidor do QRadar Packet Capture com o tempo do sistema do QRadar Console" na página 5
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 4. Cluster

Use o dispositivo QRadar Packet Capture como um único servidor independente ou como um cluster de servidores.

As edições de 10 G suportam clusters que expandem a capacidade geral de armazenamento de dados e a capacidade computacional em comparação a um único servidor independente. Os clusters contêm um principal. É possível conectar até dois dispositivos de nó de dados do QRadar Packet Capture a cada sistema principal do QRadar Packet Capture.

A guia **Cluster** exibe dois nós de dados, junto a seus status atuais.

Os nós de dados não fazem parte do cluster por padrão e possuem um status de desativado.

Ativando nós de dados

Depois de conectar fisicamente os Nós de dados do IBM Security QRadar Packet Capture ao modo principal do QRadar Packet Capture, deve-se ativar os Nós de dados do QRadar Packet Capture. Os Nós de dados do QRadar Packet Capture ativados e conectados criam um cluster para a capacidade de armazenamento incluída e o desempenho de captura aprimorado.

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

Antes de Iniciar

Certifique-se de que o Capture Server esteja em execução.

Procedimento

1. Para ativar nós de dados, siga estas etapas:
   a. Na guia **Cluster**, para cada nó de dados, selecione **Ativar**. O status mostra **Conectado**.
   b. Reinicie o Capture Server. Os Nós de Dados do QRadar Packet Capture agora estão ativados.

   Quando os Nós de dados do QRadar Packet Capture estiverem conectados e em execução, o status deles no cluster mudará para “conectado”.

   Após o nó principal se conectar um nó de dados, o tamanho de armazenamento compactado (virtual) que é exibido no painel inclui o tamanho do armazenamento dos nós de dados conectados.
2. Para desativar nós de dados, siga estas etapas:
   a. Na guia Cluster, para cada nó de dados, selecione **Desativar**. O status mostra **Desconectado**.
   b. Reinicie o Capture Server. Os Nós de dados do QRadar Packet Capture estão agora desativados e não estão mais associados ao principal.

   Um nó de dados desconectado não armazena mais dados.

   Depois que o nó principal é desativado, o tamanho do armazenamento compactado (virtual) no painel diminui.

Se Data Node1 ou Data Node2 estiver licenciado, a coluna da licença exibirá **Permanente** ou **Avaliação**, dependendo da licença usada.

Capítulo 5. Gráficos do QRadar Packet Capture

No IBM Security QRadar Packet Capture, use um gráfico em tempo real ou de histórico para visualizar estatísticas de captura de pacote.

Gráfico em tempo real

O gráfico em Tempo real controla as estatísticas de captura de pacote a seguir sobre a captura de pacote atual:

- Rendimento em Gbps (gigabits por segundo)
- Total de pacotes por segundo
- TCP_packets por segundo
- UDP_packets por segundo
- Pacotes por segundo para tráfego não UDP
- Número de eventos do sistema
- Proporção de compactação de pacote

Passe o mouse sobre o gráfico e obtenha as estatísticas para esse ponto no gráfico.

É possível clicar no gráfico em um momento e gerar uma solicitação de procura automaticamente. Também é possível clicar nos ícones de estilo de exibição para mudar a visualização do gráfico.

Gráfico de Histórico

O gráfico de Histórico fornece uma visão geral a longo prazo do histórico de captura de pacote. As opções de linha de tempo do histórico incluem 1 hora, 1 dia e 1 semana.

Passe o mouse sobre o gráfico e obtenha as estatísticas para esse ponto no gráfico.

Clique no gráfico em um momento para gerar uma solicitação de procura automaticamente.

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 de **Procura**.

   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. Na coluna **Ação** da página de procura, use a opção **Divisão em partes** para dividir solicitações de procura em segmentos de dados menores para que seja possível acessar dados enquanto a solicitação de procura inteira ainda está em execução. Solicite uma procura especificando primeiramente o número do arquivo PCAP e, em seguida, clicando em **Fazer download do arquivo PCAP**.

   Os segmentos de dados são de 128 MB e o último segmento de dados pode ser de qualquer tamanho menor que 128 MB.
8. Para ver o estado da fila de procura, visualize a **Fila de solicitações de procura**.

9. Para ver um histórico de todas as procuras concluídas, visualize o **Log de solicitações**.
10. 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. Configurando filtros de pré-captura

Filtros de pré-captura filtram o tráfego de rede antes de gravar os dados capturados no disco.

Procedimento

1. Crie um filtro de pré-captura.
   a. Clique no menu **Filtro de pré-captura**.
   b. Insira as configurações para as opções Nome do filtro e Filtro de procura.

      Um filtro de captura assume a forma de expressões primitivas que são conectadas por conjunções (e/ou) e, opcionalmente, precedidas por não.

      No exemplo a seguir, todo o tráfego destinado para a porta 80 é descartado:

      ```
      not dst port 80
      ```

      No exemplo a seguir, somente o tráfego para esses dois hosts é capturado e todo o outro tráfego é descartado:

      ```
      host 1.2.3.4 or host 1.1.1.1
      ```

   c. Conclua o filtro de pré-captura clicando em **Incluir**. O último filtro de pré-captura incluído na lista é o filtro ativo. O histórico de filtros anteriores também é exibido.
2. Reinicie o Capture Server para ativar o filtro recém-incluído.
3. Exclua o filtro permanentemente selecionando **Excluir**. Deve-se reiniciar o Capture Server.

Capítulo 8. Configurando acionadores ativos

Os acionadores ativos alertam quando ocorre um evento especificado na rede. Por exemplo, você especifica um endereço IP como o filtro de procura para ser alertado quando tráfego que contém o endereço IP é capturado.

Procedimento

1. Crie um acionador ativo.
   a. Clique no menu **Acionador ativo**.
   b. Insira as configurações para as opções Nome do acionador e Prazo.
   c. Conclua o acionador ativo clicando em **Incluir**.

   Restrição: É possível especificar até cinco acionadores ativos.
2. Revise os eventos acionadores no **Log de eventos** quando ocorrerem. Clicar em um evento acionador ativo gera automaticamente uma solicitação de procura dentro dos parâmetros de horário especificados em torno do evento acionado. O horário de procura inclui segundos antes e segundos após o evento.
3. Exclua o acionador configurado selecionando **Excluir**.

Capítulo 9. 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 versão mais recente do software QRadar Packet Capture está instalada?

Sempre faça upgrade para a versão de liberação mais recente do software. Imediatamente após aplicar uma atualização de software ou após qualquer nova instalação, certifique-se de reiniciar o sistema de forma que as mudanças sejam aplicadas. Em configurações de cluster, certifique-se de sempre de que ambos os sistemas do nó principal e de todos os nós de dados sejam atualizados para a mesma versão.

Você possui o firmware sugerido para o controlador RAID e para os discos rígidos?

Se você encontrar problemas de confiabilidade ou desempenho relacionados à revisão do firmware instalada no controlador e nos discos rígidos do RAID 3650 M4, assegure-se de ter as revisões mínimas do firmware:

- Para o 3650 M4, a revisão do firmware do controlador do RAID M5200: versão 24.7.0-0052 em 27 de maio de 2015 ou posterior.

  Execute os arquivos `.bin` a partir da linha de comandos do Red Hat Linux.
- Para IBM Lenovo, a revisão de 15 de maio de 2015 ou posterior.

  Execute os arquivos `.bin` a partir da linha de comandos do Red Hat Linux.

O Hyper-Threading (HT) está ativado no BIOS?

O HT está ativado no sistema BIOS por padrão. Execute o comando `lscpu` e revise a saída para assegurar-se de que “Encadeamento(s) por núcleo sejam iguais a 2”. Aqui está a saída de amostra do comando para o IBM 3650-M4:

```
[root@3650M4-001 bin]# lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                40
On-line CPU(s) list:   0-39
Thread(s) per core:    2
Core(s) per socket:    10
Socket(s):             2
NUMA node(s):          2
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 62
Stepping:              4
CPU MHz:               2800.000
BogoMIPS:              5592.04
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              25600K
NUMA node0 CPU(s):     0-9,20-29
NUMA node1 CPU(s):     10-19,30-39
```

A porta de captura está conectada corretamente?

O dispositivo IBM Security QRadar Packet Capture pode capturar apenas na Interface 0.

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.

O Nó de dados do QRadar Packet Capture está ativado?

Quando o Nó de dados do QRadar Packet Capture está fisicamente conectado com o nó principal, deve-se também assegurar que ele esteja ativado na interface com o usuário para trabalhar com o servidor principal. O sistema suporta atualmente até dois Nós de dados do QRadar Packet Capture.

Se a tabela **Cluster** mostra que os Nós de dados do QRadar Packet Capture estão conectados e ativados, e a configuração do **ID do sistema** está ausente da tela **Atualizar licença de nós** na guia **Administrador**, deve-se assegurar que o Nó de dados específico do QRadar Packet Capture tenha a mesma versão de software do

Nó de dados do QRadar Packet Capture instalado como o nó principal. Assegure-se de que este requisito seja atendido após atualizar para a versão de software mais recente.

Como usuário `root`, execute o comando a seguir para verificar a versão do software que está instalada no Nó de dados do QRadar Packet Capture e no nó principal:

```
cat /root/version.txt
```

A versão de software do Nó de dados do QRadar Packet Capture deve ser a mesma versão que a instalada no nó principal.

Como a licença para o Nó de dados do QRadar Packet Capture é aplicada na linha de comandos?

Para assegurar que você está no Nó de dados do QRadar Packet Capture, como usuário `root`, execute o comando a seguir:

```
cat /root/version.txt
```

Para verificar se você está conectado no Nó de dados do QRadar Packet Capture, procure um D que está anexado no final do número da versão, por exemplo, 7.2.7.256D.

Para aplicar a licença ao Nó de dados do QRadar Packet Capture, como um usuário `raiz`, execute o script: `nc_set_license.sh` como `root`.

Observações:

- Para tornar a nova licença efetiva, deve-se reiniciar o Nó de dados do QRadar Packet Capture.
- Se o Nó de dados do QRadar Packet Capture já é licenciado no momento da manufatura, você não tem que executar o script. A licença torna-se efetiva tão logo o sistema é iniciado.

Se a licença que você aplicou não é válida, uma mensagem de erro é exibida:

```
Warning: LicenseKey is *NOT* valid.
```

Qual é o formato da criação de log de LEEF 2.0?

As mensagens de LEEF (Formato estendido de evento de log) são incluídas no arquivo `/var/log/messages` no formato a seguir:

```
<DateTime> <ServerIP> LEEF: 2.0|IBM|QRadar Packet
Capture|7.2.7.256|<ID>|cat=<category> msg=<message>
```

Por exemplo, quando o servidor de captura de pacote é iniciado em um sistema que possui um endereço IP 10.91.170.20, a mensagem de LEEF a seguir é incluída no arquivo `/var/log/messages`:

```
May 24 22:27:49 IP_10_91_170_20 LEEF: 2.0|IBM|QRadar Packet
Capture|7.2.7.256|Started|cat=PacketCapture
```

Por que a solicitação Criar procura retorna um erro NoSpace ?

Se o diretório /extraction fica cheio ao criar uma procura, o servidor retorna o erro NoSpace.

O que acontece quando uma procura é pausada?

Uma procura é pausada quando o espaço usado no diretório /extraction excede 6,7 GB. Uma mensagem de LEEF é enviada para Syslog indicando que a procura está pausada. O log de eventos exibe um aviso semelhante a:

```
!WARNING: Extraction Storage Full! Search cannot proceed!!
```

Para assegurar que uma procura pausada seja retomada, deve-se criar espaço excluindo as procuras mais antigas, concluídas anteriormente. Para excluir uma procura antiga, siga as etapas a seguir:

1. Clique na opção de menu principal **Procura**.
2. No quadro **Log de solicitação de procura**, exclua as procuras antigas clicando em **Excluir procura**.

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

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.

Quaisquer 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 nesses websites não fazem parte dos materiais deste produto IBM e o uso desses websites é de total 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
Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Av. Pasteur, 138/146 - Botafogo
Rio de Janeiro, RJ
Estados Unidos

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.

Os dados de desempenho e os exemplos dos clientes citados são apresentados para fins ilustrativos apenas. Resultados reais de desempenho podem variar dependendo de configurações específicas e condições operacionais.

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.

As declarações relacionadas a direção ou intenção futuros da IBM estão sujeitas a alteração ou retirada sem aviso prévio e representam metas e objetivos apenas.

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 esses nomes são fictícios e qualquer semelhança com empresas ou pessoas reais é mera coincidência.

Marcas comerciais

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas comerciais da International Business Machines Corp., registradas em muitas jurisdições no mundo inteiro. Outros nomes de produtos e serviços podem ser marcas comerciais da IBM ou outras empresas. Uma lista atual das marcas comerciais da IBM está disponível na web em "Informações de marca comercial e copyright" em www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT e o logotipo Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos, outros países ou ambos.

Termos e condições para a documentação do produto

Permissões para o uso dessas publicações são concedidas de acordo com os seguintes termos e condições.

Aplicabilidade

Esses termos e condições estão completando quaisquer termos para uso do website IBM.

Uso pessoal

Você pode reproduzir estas publicações para seu uso pessoal, não comercial, desde que todos os avisos do proprietário sejam preservados. Você não pode distribuir, exibir ou fazer trabalho derivado dessas publicações, ou qualquer parte delas, sem o consentimento expresso da IBM.

Uso Comercial

É possível reproduzir, distribuir e exibir essas publicações unicamente dentro de sua empresa, contanto que todos os avisos do proprietário sejam preservados. Não é permitido criar trabalhos derivados destas publicações, ou reproduzir, distribuir ou exibir estas publicações ou qualquer porção das mesmas fora de sua empresa, sem o consentimento expresso da IBM.

Direitas

Exceto conforme expressamente concedido nessa permissão, nenhuma outra permissão, licença ou direito é concedido, seja expresso ou implícito, às publicações ou quaisquer informações, dados, software ou outra propriedade intelectual contida neste.

A IBM reserva-se o direito de retirar as permissões concedidas neste documento sempre que, a seu critério, o uso das publicações for prejudicial ao seu interesse ou, conforme determinado pela IBM, as instruções acima não estiverem sendo seguidas da maneira adequada.

O Cliente não pode fazer download, exportar ou reexportar estas informações, exceto se elas estiverem totalmente em conformidade com todas as leis e regulamentações aplicáveis, incluindo todas as leis e regulamentações de exportação dos Estados Unidos.

A IBM NÃO SE RESPONSABILIZA PELO CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS "NO ESTADO EM QUE SE

ENCONTRAM" E SEM GARANTIA DE QUALQUER TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E DE ADEQUAÇÃO PARA UM PROPÓSITO ESPECÍFICO.

Declaração de privacidade on-line da IBM

Os produtos do software IBM, incluindo as soluções de software como serviço, (“Ofertas de software”) podem usar cookies ou outras tecnologias para coletar informações do uso do produto, para ajudar a melhorar a experiência do usuário final, para 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 pessoais identificáveis, informações específicas sobre o uso de cookies desta oferta serão estabelecidas a seguir.

Dependendo das configurações implementadas, essa Oferta de Software poderá usar cookies de sessão que coletam o ID da sessão de cada usuário para fins de gerenciamento de sessões e autenticação. Estes cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade que eles ativam.

Se as configurações implementadas para esta Oferta de Software fornecerem a capacidade de coletar, como cliente, informações pessoalmente identificáveis dos usuários finais por meio de cookies e outras tecnologias, deve-se consultar seu próprio conselho jurídico a respeito das leis aplicáveis a essa 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 em http://www.ibm.com/privacy/details, a seção intitulada “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.

Impresso no Brasil