IBM Security QRadar Incident Forensics
Versão 7.3.0

QRadar Packet Capture Guia de consulta rápida

Nota

Antes de usar estas informações e o produto que ela suporta, leia as informações em “Avisos” na página 7.

Informações do produto

Este documento aplica-se ao IBM QRadar Security Intelligence Platform V7.3.0 e às liberações subsequentes, a não ser que seja substituído por uma versão atualizada.

Índice

Sobre este guia de consulta rápida do Packet Capture v

Capítulo 1. Atualizando o QRadar Packet Capture. 1

Capítulo 2. Referência rápida do QRadar Packet Capture 3

Avisos 7
Marcas comerciais 9
Termos e condições para a documentação do produto 9
Declaração de privacidade on-line da IBM 10

Sobre este guia de consulta rápida do Packet Capture

Esta documentação fornece informações de referência rápida que serão necessárias para instalar e configurar o IBM® Security QRadar Packet Capture. O QRadar Packet Capture é suportado pelo IBM Security QRadar.

Público desejado

Administradores do sistema responsáveis pela instalação do QRadar Packet Capture devem estar familiarizados com os conceitos de segurança de rede e configurações do 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. Atualizando o QRadar Packet Capture

Para fazer upgrade do QRadar Packet Capture V7.2.8 para o V7.3.0, instale um fix pack de software acumulativo em um dispositivo QRadar Packet Capture. A versão do software que é instalada no dispositivo deve ser a construção 7.2.6.241.

Procedimento

1. Assegure-se de que não haja atividades de captura de pacote ou procura em andamento.
2. Use SSH para efetuar login no sistema como usuário `root`.
3. Faça download do fix pack `7.3.0-QRadar-PCAP-build<build_number>.sfs` a partir do IBM Fix Central (http://www.ibm.com/support/fixcentral/)
4. Copie o fix pack para o diretório `/tmp`.

   Se o espaço no diretório `/tmp` for limitado, copie o fix pack em outro local que tenha espaço suficiente.
5. Crie o diretório `/updates` digitando o comando a seguir:

   ```
   mkdir -p /updates
   ```
6. Use o comando **cd** para mudar para o diretório no qual você copiou o arquivo de fix pack.

   ```
   cd /tmp
   ```
7. Para montar o arquivo de fix pack no diretório `/updates`, digite o comando a seguir:

   ```
   mount -o loop -t squashfs 7.3.0-QRadar-PCAP-build<build_number>.sfs
   /updates
   ```
8. Para executar o instalador do fix pack, mude o diretório para `/updates` e digite o comando a seguir:

   ```
   sh installer.sh
   ```
9. Reinicie o sistema.

Capítulo 2. Referência rápida do QRadar Packet Capture

Antes de ser possível capturar pacotes, deve-se definir as configurações de conexão e de rede do IBM Security QRadar Packet Capture.

Lista de compatibilidade de Intel SFP+ e SFP

O dispositivo QRadar Packet Capture possui somente uma porta de captura (DNA0). O dispositivo QRadar Packet Capture não está equipado com um transceptor SFP, portanto, deve-se instalar um SFP+ 10G ou SFP 1G (RJ45 de Cobre) na porta de captura.

Para comprar módulos SFP para o seu dispositivo QRadar Packet Capture, consulte os websites de fornecedor a seguir:

- Website do Digi-Key (http://www.digikey.com)
- Website do Mouser Electronics (http://www.mouser.com)
- Website do CDW (http://www.cdw.com)
- Website do Newegg (https://www.newegg.com)
- Website do Amazon (http://amazon.com)

Quando o SFP 1G é instalado, ele trunca a taxa de captura em 1 Gbps.

Para ter várias conexões de 1G, é possível colocar um comutador ou um agregador na frente de onde a porta de saída do 10G vai para a porta do QRadar Packet Capture SFP+ 10G. Como resultado, é possível ter várias portas de 1 Gb agregadas na interface do QRadar Packet Capture 10G SFP+.

A lista a seguir descreve os requisitos dos módulos SFP+ e SFP:

Número de Peça	**Descrição**
E10GSFPSR	Taxa dual 10GBASE-SR/1000BASE-SX, Intel Ethernet SFP+ SR ótico
E10GSFPLR	Taxa dual 10GBASE-LR/1000BASE-LX, Intel Ethernet SFP+ LR ótico
FCLF8522P2BTL	1000BASE-T, Transceptor Finisar Gigabit Ethernet
453153-001	Transceptor HP Gigabit SX

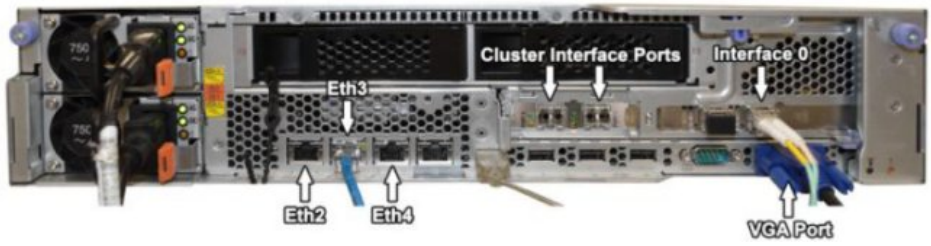
Configuração de rede

Para configurar inicialmente a rede, são necessários uma tela, um teclado e uma conexão Ethernet com uma porta integrada. Por padrão, o sistema possui portas DHCP ativas.

Se você souber o endereço IP da porta Ethernet que está em uso, acesse Iniciar gravação.

1. Forneça uma conexão de rede para acesso remoto com o servidor.

Forneça uma conexão Ethernet com uma das portas Ethernet integradas, eth2, eth3 ou eth4, conforme mostrado no diagrama a seguir.



2. Forneça uma conexão de rede para captura de rede.

   Forneça conexões 10G de fibra usando as portas da Interface 0 mostradas no diagrama a seguir.

   Importante: Assegure-se de que haja tráfego sobre as conexões. Para capturar o tráfego, deve-se usar uma porta Tap ou SPAN (espelho). Quando você usa uma porta SPAN em um comutador, se o comutador designar uma prioridade inferior à porta SPAN, alguns pacotes poderão ser eliminados.

3. Use SSH e porta 4477 para efetuar login como usuário raiz.

   O nome do usuário padrão é: `root`. A senha padrão é: `P@ck3t08..`

4. Registre o endereço IP.

   Após o login, abra um terminal e insira o comando a seguir: `#ifconfig -a`

   Esse comando fornece o endereço IP da porta Ethernet que está conectada.

   Nota: Para obter informações sobre como configurar um endereço IP estático, consulte o *IBM Security QRadar Packet Capture User Guide.*

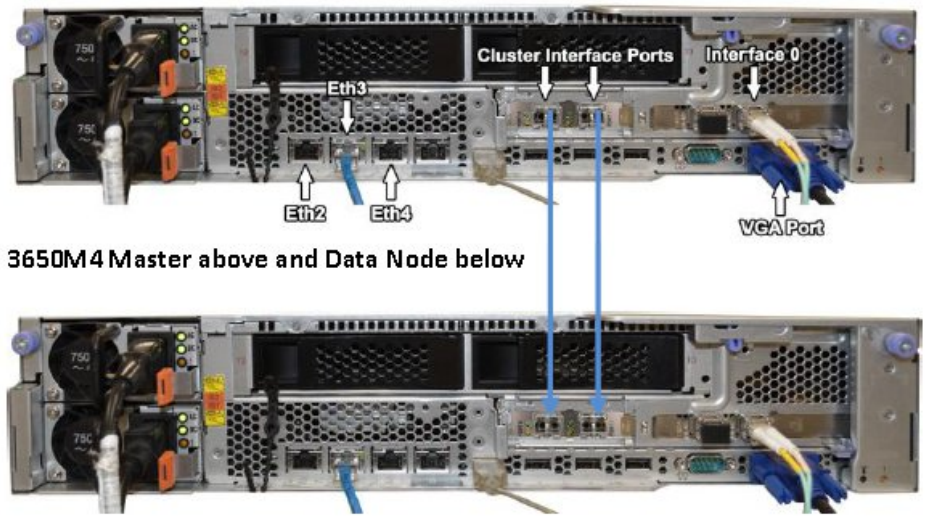
5. Teste a conexão.

   Para testar a conexão, execute ping da rede interna ou efetue login remotamente usando SSH na porta 4477. Assegure-se de que haja uma conexão bem-sucedida antes de continuar.

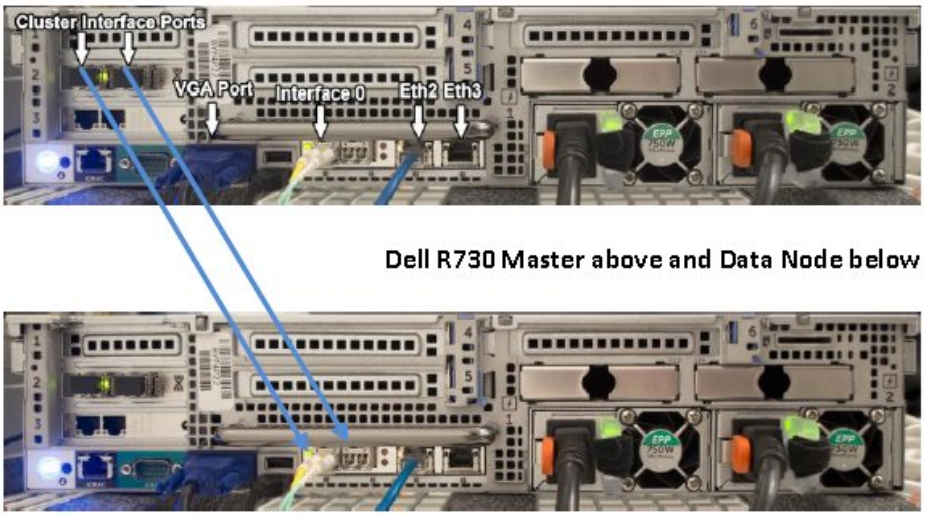
Conectar o cluster

Após conectar a rede ao sistema principal ou independente com êxito, conecte o dispositivo de captura de pacote principal aos dispositivos do QRadar Packet Capture Data Node. Se você tiver somente um sistema de captura de pacote independente, esta etapa não será necessária.

1. Consulte o diagrama de hardware para seu dispositivo de captura de pacote.
   - Conexão do dispositivo de captura de pacote principal IBM System x3650 M4 e do QRadar Packet Capture Data Node



- Dispositivo de captura de pacote Dell R730 e QRadar Packet Capture Data Node



2. Na parte traseira do dispositivo de captura de pacote, conecte a porta de interface do cluster esquerdo no principal à porta de interface do cluster esquerdo no primeiro nó de dados, conforme indicado pelas setas nos diagramas anteriores.
3. Se houver um segundo nó de dados, conecte a porta de interface do cluster direito no principal à porta de interface direita no segundo nó de dados.
4. A partir de um terminal no sistema principal, verifique as conexões com um teste de ping:

   ```
   ping 1.1.1.2
   ping 2.2.2.2
   ```

5. Se você não receber uma resposta do ping, troque as conexões dos cabos somente nas interfaces do nó de dados.
   - Se somente um nó de dados estiver conectado, somente um ping deverá responder com êxito.
   - Se após a troca dos cabos ainda não houver nenhuma resposta do teste de ping, troque os cabos na NIC do nó de dados para a segunda NIC de Ethernet óptica instalada (se houver uma) e repita o teste de ping.

Iniciar gravação

Depois de haver uma conexão de rede bem-sucedida com o sistema, é possível iniciar a gravação de pacotes de rede no disco e visualizar estatísticas sobre tráfego em uma rede.

1. Abra um navegador da web e acesse o dispositivo:

   `https://PCAP_IP_Address:41390`
2. Efetue login usando as informações sobre o usuário:

   User: `continuum`

   Password: `P@ck3t08..`
3. Ative cada nó de dados (escravo) conectado fisicamente.
4. Inicie a gravação.

   Após efetuar login e ativar os nós de dados, acesse a página **Estado da captura** e clique em **Iniciar captura**.

   Nota: Após o início da captura, é exibida uma janela de estatísticas contendo todos os detalhes de captura.

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.

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