IBM Security QRadar
Versão 7.2.5

Packet Capture: Guia de consulta rápida

Nota

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 5.

Informações do produto

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

Índice

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 SIEM.

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 de 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 a Nota técnica sobre 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 dos sistemas e de informações por meio de prevenção, detecção e resposta a acesso incorreto de dentro e fora da empresa. O acesso incorreto pode resultar em informações sendo alteradas, destruídas, desapropriadas ou usadas indevidamente ou pode resultar em danos ou uso impróprio dos sistemas, incluindo uso em ataques a outros. Nenhum sistema ou produto de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança sozinha pode ser completamente efetiva na prevenção de uso ou acesso impróprios. Sistemas, produtos e serviços IBM são projetados para fazer parte de uma abordagem de segurança abrangente legal, que necessariamente envolverá procedimentos operacionais adicionais, podendo requerer outros sistemas, produtos ou serviços para ser mais eficiente. A IBM NÃO GARANTE QUE OS SISTEMAS, PRODUTOS OU SERVIÇOS ESTEJAM IMUNES OU TORNEM SUA EMPRESA IMUNE CONTRA A CONDUTA MAL-INTENCIONADA OU ILEGAL DE QUALQUER PARTE.

Observe:

O uso deste Programa pode implicar várias leis ou regulamentos, incluindo aqueles relacionados à privacidade, à proteção de dados, à empregabilidade, às comunicações eletrônicas e ao armazenamento. O IBM Security QRadar pode ser usado somente para propósitos legais e de uma forma legal. O cliente acorda em usar este Programa conforme as políticas, os regulamentos e as leis aplicáveis e assume toda a responsabilidade por sua conformidade com estes. O licenciado declara que obterá ou obteve quaisquer licenças, permissões ou consentimentos necessários para possibilitar seu uso do IBM Security QRadar.

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 um transceptor 10G, consulte a página da web da Digi-Key (http://www.digikey.com/product-detail/en/FTLX8571D3BCL/775-1060-ND/1967719?WT.srch=1&WT.medium=cpc&WT.mc_id=IQ66882673-VQ2-g-VQ6-45013742355-VQ15-1t1-VQ16-c).

Para comprar um transceptor 1G, consulte a página da web da Digi-Key(http://www.digikey.com/product-detail/en/FCLF-8521-3/775-1003-ND/1832807)

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 do módulo SFP+ e SFP para o Intel Ethernet Converged Network Adapter X520 Series:

- O Intel Ethernet SFP+ SR Optics e o Intel Ethernet SFP+ LR Optics são os únicos módulos óticos de 10 Gbps suportados e é possível comprar estes módulos separadamente.
- Outras marcas de módulos SFP+ (10 Gbps) não são permitidas e não podem ser usadas com estes adaptadores.
- Os adaptadores -SR incluem o Intel Ethernet SFP+ SR Optics.
- O adaptador -LR inclui um Intel Ethernet SFP+ LR Optic.
- O adaptador -DA2 não inclui qualquer módulo SFP+ ou SFP.
- Conforme mostrado na tabela a seguir, alguns módulos 1000BASE-T e 1000BASE-SX funcionam com o Intel Ethernet Converged Network Adapter X520 Series.

Tabela 1. Módulos 1000BASE-T e 1000BASE-SX suportados

Nome	Código do Produto ou Número de Peça	Tipo
Intel Ethernet SFP+ SR Optics	E10GSFPSR	10GBASE-SR/1000BASE-SX de Taxa Dual
Intel Ethernet SFP+ LR Optics	E10GSFPLR	10GBASE-LR/1000BASE-LX de Taxa Dual

Tabela 1. Módulos 1000BASE-T e 1000BASE-SX suportados (continuação)

Nome	Código do Produto ou Número de Peça	Tipo
Avago Gigabit Ethernet Transceiver [1]	ABCU-5710RZ	1000BASE-T
Finisar Gigabit Ethernet Transceiver [1]	FCLF8522P2BTL	1000BASE-T
HP Gigabit SX Transceiver [1]	453153-001	
[1] Não pode ser testado		

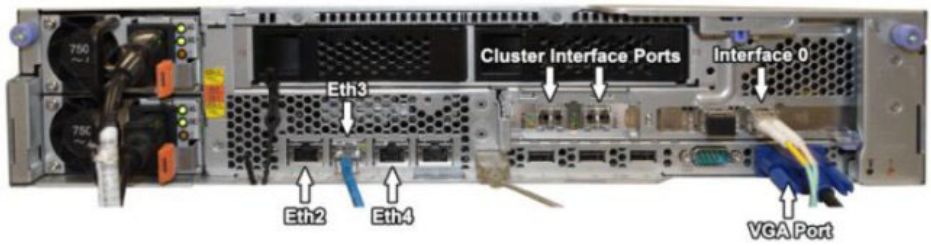
Configuração de rede

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 para efetuar login.

   Depois de iniciar o sistema, efetue login usando as informações sobre o usuário a seguir:

   User: `continuum`

   Password: `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.

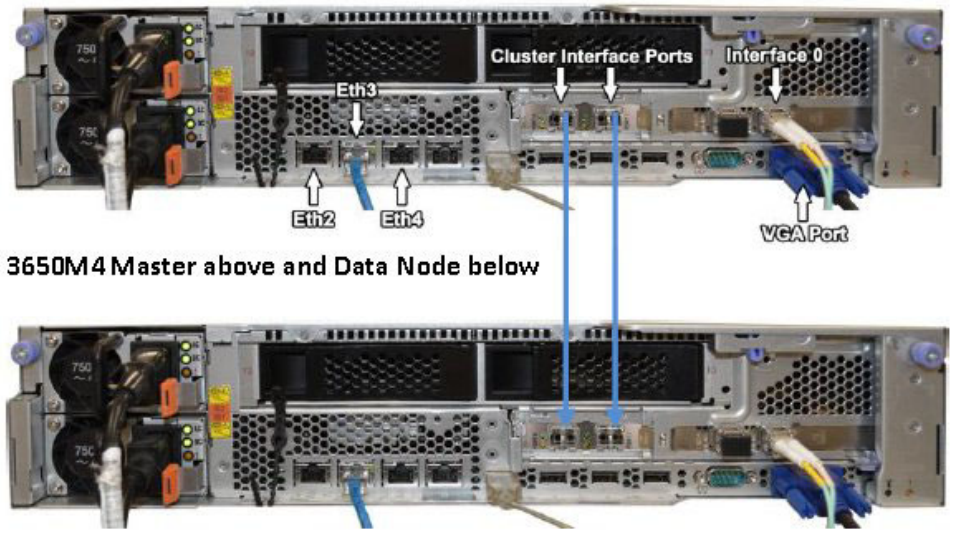
   Para testar a conexão, execute ping da rede interna ou efetue login remotamente usando SSH na porta 4477. Assegure-se de que haja uma conexão bem-sucedida antes de continuar.

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



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. Em 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. Inicie a interface da web.

   Em qualquer sistema remoto conectado à rede, abra um navegador da web e insira o endereço IP seguido de `/login.html`

   Exemplo: `http://192.168.1.1/login.html`
2. Efetue login.

   A tela de login do QRadar Packet Capture é exibida.

   É criada uma conta padrão.

   Insira o nome de usuário e a senha a seguir:

   User: `continuum`

   Password: `P@ck3t08..`

   Na primeira vez que você efetuar login, será solicitado para alterar a senha.
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

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 sobre a política de privacidade

Produtos de software IBM, incluindo soluções de software como serviço, (“Ofertas de Software”) podem usar cookies ou outras tecnologias para coletar informações de uso do produto, ajudar a melhorar a experiência do usuário final, customizar interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação de identificação pessoal é coletada pelas Ofertas de software. Algumas de nossas Ofertas de software podem ajudá-lo a coletar informações de identificação pessoal. Se esta Oferta de software usar cookies para coletar informações de identificação pessoal, informações específicas sobre o uso de cookies desta oferta serão estabelecidas 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 e autenticação de sessões. Esses cookies podem ser desativados, mas sua desativação também eliminará a funcionalidade ativada.

Se as configurações implementadas para esta Oferta de software fornecerem a você como cliente a capacidade de coletar informações de identificação pessoal de usuários finais por meio de cookies e outras tecnologias, você deverá consultar seu próprio conselho jurídico sobre as leis aplicáveis a essa coleta de dados, incluindo requisitos para 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, na seção intitulada “Cookies, web beacons e outras tecnologias” e a “Declaração de privacidade de software como serviço e produtos de software IBM” em http://www.ibm.com/software/info/product-privacy.