CA Nimsoft Monitor para Flow Analysis

Guia do Usuário

Release 1.1

Histórico da revisão do documento

Versão do documento	Data	Alterações
1.1	11/30/2012	Atualizado para a release 1.1 do Flow Analysis. Adicionado intervalo de tempo personalizado para relatórios, explicação de intervalos de relatórios de dados e outras alterações secundárias.
1.0	9/10/2012	Guia do Usuário da Versão Inicial do *CA Nimsoft Monitor para Flow Analysis*

Entre em contato com a CA Nimsoft

Entrar em contato com a CA Support

Para sua conveni_ncia, a CA Technologies oferece um site onde _ poss_vel acessar as informa__es necess_rias a seus produtos da CA Technologies para escrit_rio dom_stico, pequena empresa e corporativos. Em http://www.ca.com/worldwide, _ poss_vel acessar os seguintes recursos:

- Informa__es para contato online e telef_nico, assist_ncia t_cnica e atendimento ao cliente
- Informa__es sobre f_runs e comunidades de usu_rio
- Downloads de produto e documenta__o
- Pol_ticas e diretrizes de CA Support
- Outros recursos _teis adequados ao seu produto

Fornecendo coment_rios sobre a documenta__o do produto

Enviar coment_rios ou perguntas sobre a documenta__o de produtos da Nimsoft da CA Technologies para nimsoft.techpubs @ ca.com.

Se desejar fornecer coment_rios sobre a documenta__o geral dos produtos da CA Technologies, responda nossa breve pesquisa do cliente, dispon_vel no site de CA Support, encontrado em http://ca.com/docs.

Avisos legais

Garantia

O material contido neste documento é fornecido "como está" e está sujeito a alterações em edições futuras sem aviso prévio. Além disso, na medida permitida pela lei aplicável, a Nimsoft LLC isenta-se de todas as garantias, sejam implícitas ou expressas, com relação a este manual e todas as informações contidas no presente documento, incluindo, sem limitação, garantias implícitas de comerciabilidade e adequação para um determinado fim. A Nimsoft LLC não será responsabilizada por erros ou danos acidentais ou resultantes do fornecimento, uso ou desempenho deste documento ou de qualquer outra informação contida no presente. Caso a Nimsoft LLC e o usuário tenham um acordo por escrito à parte sobre termos de garantia que cobrem o material deste documento conflitando com estes termos, os termos de garantia do acordo à parte prevalecerão.

Licenças de tecnologia

O hardware e/ou software descritos neste documento são fornecidos sob uma licença e poderão ser usados ou copiados somente de acordo com os termos da referida licença.

Nenhuma parte deste manual poderá ser reproduzida de qualquer forma ou por qualquer meio (incluindo a recuperação e o armazenamento eletrônico ou a tradução em um idioma estrangeiro) sem um acordo prévio e consentimento por escrito da Nimsoft LLC, em conformidade com as leis de direitos autorais internacional e dos EUA.

Legenda de direitos restritos

Se o uso do software for destinado ao cumprimento de um contrato ou subcontrato do governo dos Estados Unidos da América -EUA, o software será fornecido e licenciado como "software comercial para computadores", conforme definido no DFAR 252.227-7014 (junho de 1995), ou como um "item comercial", conforme definido no FAR 2.101(a); ou como "software de computador restrito", conforme definido no FAR 52.227-19 (junho de 1987) ou em qualquer regulamento equivalente do órgão ou Cláusula contratual. O uso, a duplicação ou a divulgação do software está sujeito aos termos de licença comercial padrão da Nimsoft LLC, os departamentos que não fazem parte do DOD (Department of Defense) e os órgãos do governo dos EUA não receberão mais Direitos do que os Direitos Restritos, conforme definido no FAR 52.227-19(c)(1-2) (junho de 1987). Os usuários do governo dos EUA não receberão mais que Direitos Limitados, conforme definido no FAR 52.227-14 (junho de 1987) ou no DFAR 252.227-7015 (b)(2) (novembro de 1995), conforme aplicável em quaisquer dados técnicos.

Marcas registradas

Nimsoft é uma marca registrada da CA.

Adobe®, Acrobat®, Acrobat Reader® e Acrobat Exchange® são marcas registradas da Adobe Systems Incorporated.

Intel® e Pentium® são marcas registradas da Intel Corporation dos EUA.

Java(TM) é uma marca registrada da Sun Microsystems, Inc. dos EUA.

Microsoft® e Windows® são marcas registradas da Microsoft Corporation dos EUA.

Netscape(TM) é uma marca registrada da Netscape Communications Corporation dos EUA.

Oracle® é uma marca registrada da Oracle Corporation, Redwood City, Califórnia, Estados Unidos.

UNIX® é uma marca registrada do Open Group.

ITIL® é uma marca comercial registrada do Office of Government Commerce no Reino Unido e em outros países.

Todas as marcas comerciais, nomes comerciais, marcas de serviços e logotipos mencionados neste documento pertencem às respectivas empresas.

Para obter informações sobre software de domínio público e licença, consulte a *Licença de Terceiros e Termos de Uso do Nimsoft Monitor* do documento no site: http://docs.nimsoft.com/prodhelp/en_US/Library/index.htm?toc.htm?1981724.html.

Índice

Capítulo 1: Introdução

Esta seção contém os seguintes tópicos:

Sobre este guia

Este guia o ajuda a obter o máximo benefício do CA Nimsoft Monitor para a solução do Flow Analysis. O guia contém as seguintes seções:

- **Introdução** -- Informações sobre este guia e uma introdução aos conceitos do Flow Analysis
- **Guia rápido** -- Abrange as etapas necessárias para iniciar o uso do Flow Analysis
  - Componentes de pré-requisito
  - Configurar o portlet Gerador de relatórios
  - Configuração -- Abrange as tarefas de configuração necessárias para:
    - Roteadores e acesso à porta que fornecem dados de fluxo de rede
    - Sistema do Coletor e probe do Flow Analysis
    - Portlet e interface gráfica do usuário do Flow Analysis
- **Relatórios** -- descreve a interface gráfica do usuário do Flow Analysis, seus controles, e os relatórios de fluxo de dados que estão disponíveis
- **Solução de problemas** -- descreve problemas do uso do produto e suas soluções

Conceitos do Flow Analysis

O Flow Analysis foi desenvolvido para integrar a exibição do fluxo de tráfego pela rede com os dados e alarmes de QoS, todos exibidos no Nimsoft UMP (Unified Management Portal). Com o Flow Analysis, você pode:

- Identificar imediatamente as interfaces, hosts e os aplicativos que geram a maior parte do tráfego em sua empresa. Essa informação é essencial para a solução de problemas de curto e longo prazo.
- Revisar os alarmes do Nimsoft, juntamente com o fluxo de dados para identificar os problemas de rede de forma rápida.
- Analisar tendências em aplicativos, hosts e conversas por classe de serviço. Essas informações ajudam você a otimizar a infraestrutura de rede para o desempenho do aplicativo.

Terminologia do Flow Analysis

Netflow

O NetFlow refere-se aos protocolos (NetFlow versões 5, 7 e 9, bem como IPFIX, Jflow, sFlow, cflowd, Rflow e NetStream) que permitem a coleta de estatísticas de tráfego de IP em interfaces de dispositivo de rede. Um roteador está configurado para exportar informações do fluxo de dados, envio de pacotes UDP que contêm estatísticas de fluxo para um coletor.

O fluxo de informações é útil para responder aos seguintes tipos de perguntas:

- Você sabe quais são todos os aplicativos em execução na sua rede?
- Quais são os padrões de tráfego de aplicativos?
- Quais aplicativos e hosts estão consumindo a maior parte da largura de banda?
- Qual a capacidade de link que preciso no futuro? Realmente a resposta aos problemas de desempenho é maior largura de banda?

Conversa

A conversa é uma sessão de tráfego entre sub-redes ou entre usuários (entre hosts). O portal do Flow Analysis exibe esta informação -- É possível descobrir se uma determinada conversa está causando um pico de tráfego em uma interface, por exemplo, e identifica as principais conversas com base no volume.

Fluxo

Um fluxo é um conjunto de pacotes IP que passam em um ponto de observação de rede durante um certo intervalo de tempo. Um fluxo pode consistir em Flexible NetFlow, Sampled NetFlow, NetFlow v5, v7, ou v9; sFlow versão 5 ou quaisquer versões comparáveis do IPFIX, Jflow, cFlow ou NetStream.

Interface

Uma interface é um ponto de conexão, como uma interface serial, Frame Relay, Fast Ethernet, ATM ou PVC. O Flow Analysis informa sobre qualquer interface lógica ativa em um roteador suportado que tem seu fluxo ativo. O portal exibe as interfaces que são monitoradas no seu ambiente.

Protocolo

Um protocolo é um padrão para controlar a comunicação entre computadores. Os protocolos comuns incluem: HTTP, SNMP, FTP e VoIP. As informações exibidas podem incluir os principais protocolos de entrada e saída de determinada interface. Estas informações podem ajudar a identificar qual aplicativo está gerando tráfego de rede. Também é possível criar e executar relatórios a fim de determinar quais protocolos e aplicativos são usados por grupos diferentes em sua empresa.

QoS (Qualidade de serviço)

QoS (Qualidade de serviço) é um nível definido de desempenho -- qualidade de transmissão e disponibilidade do serviço -- em uma rede de dados.

Relatório

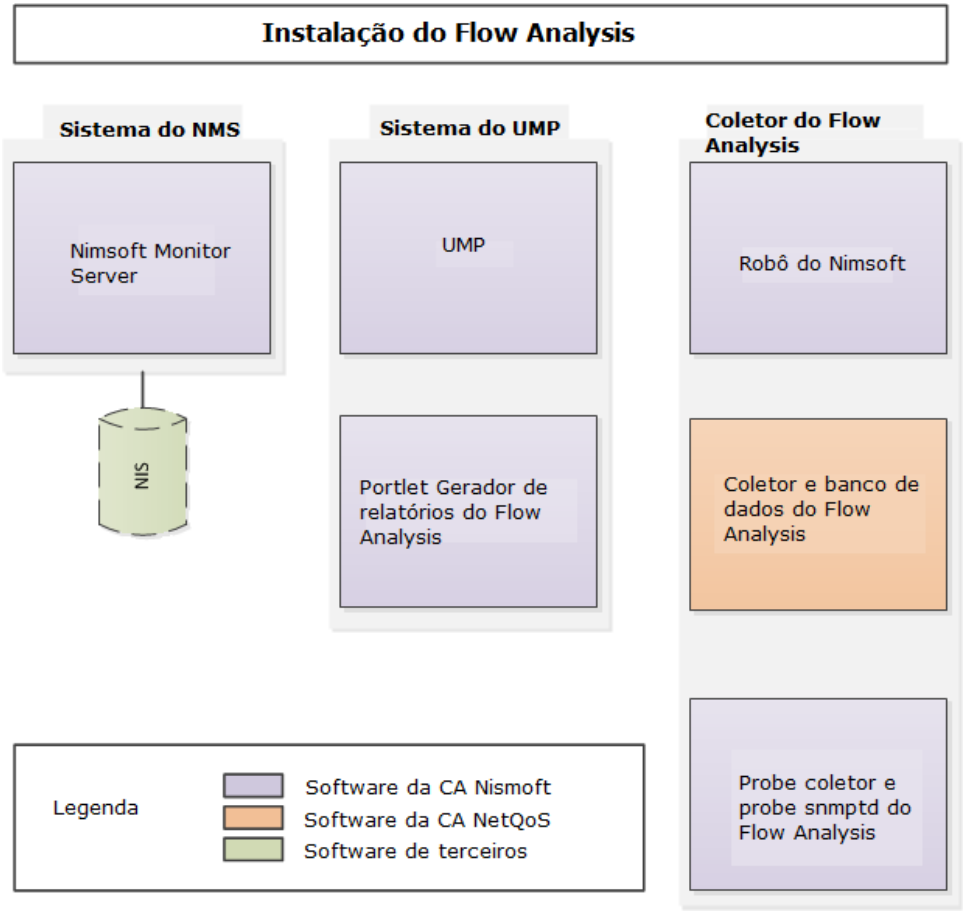
Um relatório é uma exibição dos dados coletados, que é possível ser visualizado no portlet do Flow Analysis no UMP. É possível exportar relatórios como arquivos de valores separados por vírgulas (CSV).

Capítulo 2: Introdução

Esta seção contém os seguintes tópicos:

Componentes de pré-requisito

Consulte o *Guia de Instalação do Flow Analysis* e confirme se todos os componentes de software necessários estão instalados, licenciados e operacionais:



O Flow Analysis consiste nestes componentes:

- Sistema do NMS - Banco de dados do NIS e Nimsoft Monitor Server
- Sistema do UMP - UMP (Unified Monitoring Portal) e o portlet do Reporter do Flow Analysis
- Sistema do Coletor - Banco de dados e Coletor do Flow Analysis, um robô da Nimsoft e os probes snmptd e Coletor do Flow Analysis

Observação: o coletor e o banco de dados do Flow Analysis são baseados nos produtos CA NetQoS Harvester e Reporter/Analyzer, respectivamente.

Implantar o portlet Gerador de relatórios do Flow Analysis

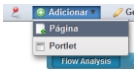
Para configurar os componentes do Flow Analysis e visualizar os relatórios de fluxo de dados, o portlet Gerador de relatórios do Flow Analysis precisa ser implantado dentro do Unified Monitoring Portal (UMP).

Para começar, siga estas etapas:

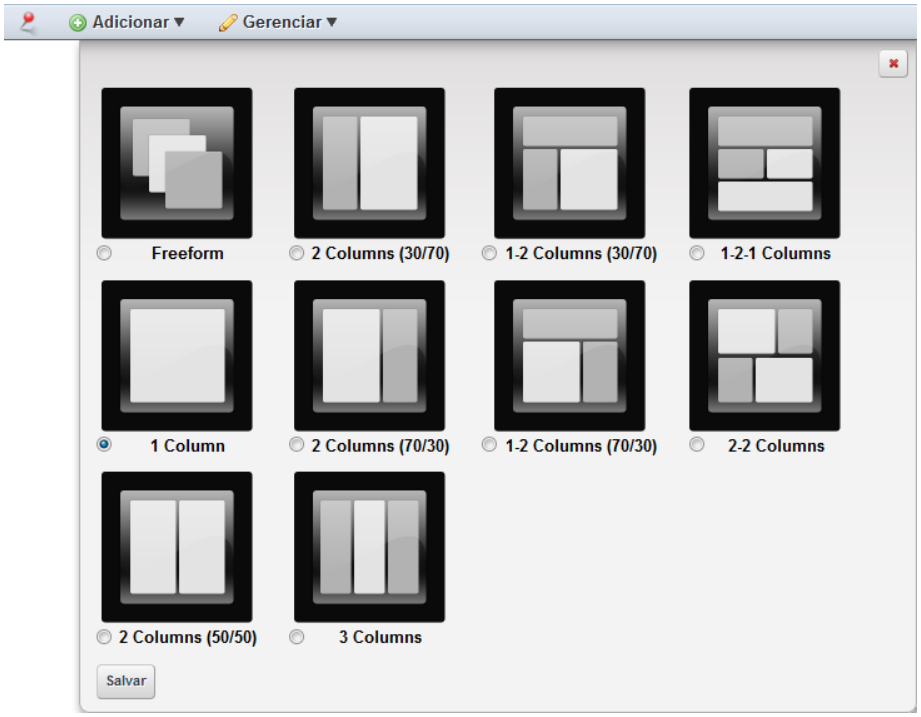
1. Confirme se o probe ump_flow foi implantado no robô do sistema UMP. Isso pode ser verificado no Gerenciador de infraestrutura. Localize o ícone do robô do sistema UMP e o ícone do probe ump_flow deve estar visível sob ele e na cor verde. Para revisar as instruções de instalação, consulte a seção Instalação do portlet Gerador de relatórios do Flow Analysis no *Guia de Instalação do Flow Analysis*).
2. Inicie o UMP (http://<IPaddress_of_UMP_system>)
3. Siga as etapas abaixo para adicionar a guia do Flow Analysis para o UMP.

   Observação: um tratamento mais completo de como configurar páginas e portais no UMP está disponível na ajuda online do UMP na seção **Bem-vindo> Introdução ao UMP**.

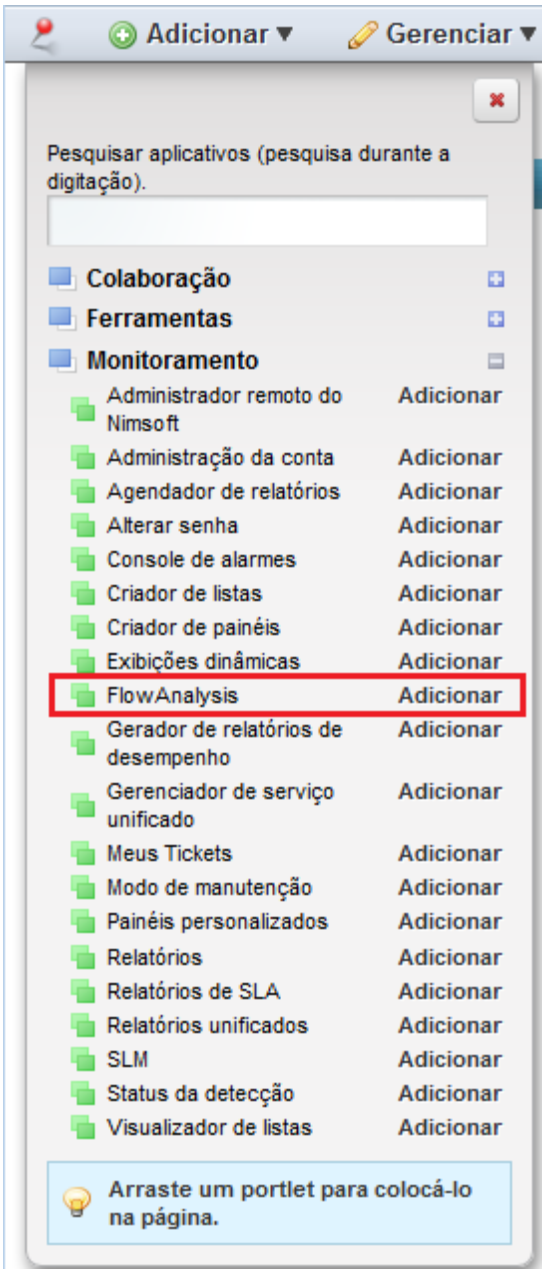
   1. Adicionar uma página vazia: na parte superior esquerda do UMP, escolha: **Adicionar > Página**, atribua um nome para a nova página (recomendamos Flow Analysis) e, em seguida, clique na caixa de seleção para confirmar e salvar.



2. Ajustar o layout da página: selecione a nova página e, em seguida, selecione **Gerenciar> Layout de Página> 1 coluna** no menu na parte superior esquerda da janela do navegador e clique em **Salvar**.



3. Instalar o portlet do Flow Analysis na nova página: escolha **Adicionar> Portlet**. Em seguida, selecione o Flow Analysis em **Monitoramento** e clique em **Adicionar**.



4. O portlet é carregado na página, inicia e encontra os coletores do Flow Analysis disponíveis. Aqueles que são localizados são exibidos na lista suspensa do Coletor no formulário "hub/robô/domínio".

Observação: o probe discovery_server deve ser executado no host do NMS para a lista suspensa do coletor exibir os coletores do Flow Analysis. Se um coletor existente não estiver listado nessa lista suspensa, talvez ele não tenha sido detectado ainda. Execute novamente a detecção no Assistente de detecção do USM para localizar outros Coletores.

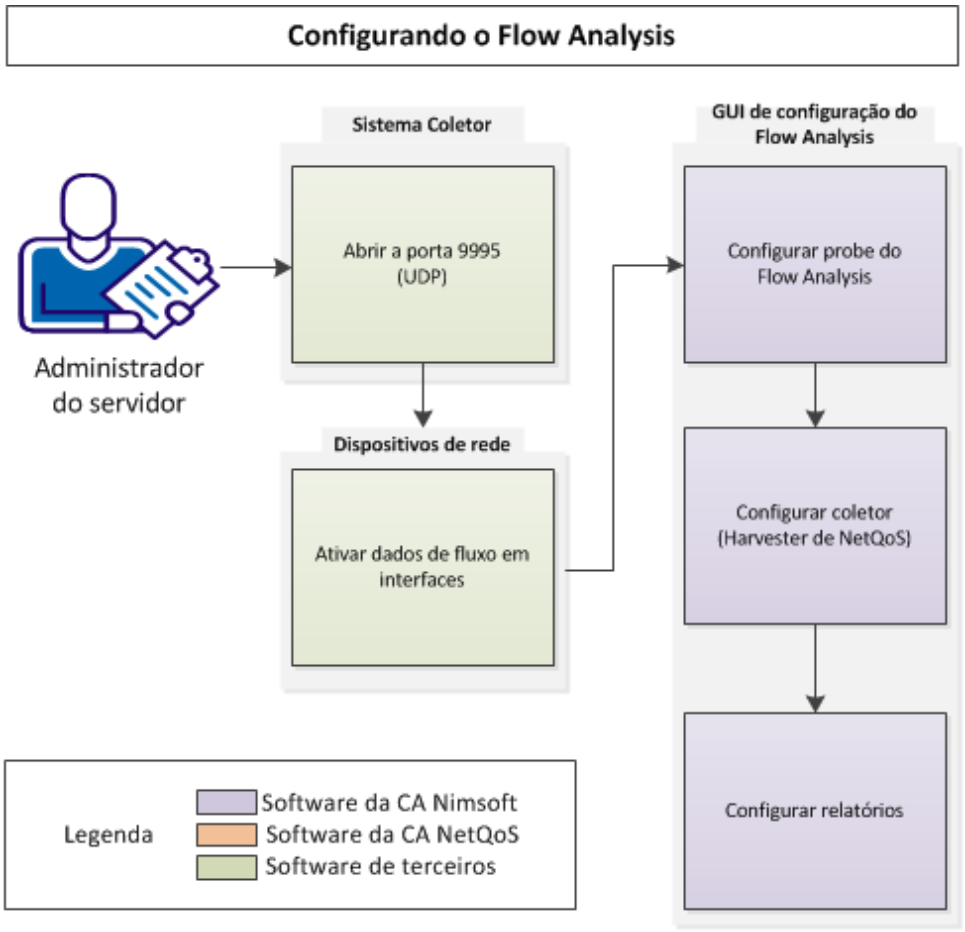
5. Selecione o coletor desejado a partir da lista suspensa.
6. A página principal do Flow Analysis exibe estes três gráficos dos dados do relatório TopN:
    1. Interfaces principais
    2. Hosts principais
    3. Aplicativos principais.

Observação: se você tiver acabado de iniciar o sistema, os dados não poderão ser exibidos até que um intervalo de quinze minutos tenha passado.

É possível detalhar os dados exibidos clicando-se nos links em azul. Consulte a seção sobre Página principal do Flow Analysis (na página 32) para obter detalhes.

Configuração

A configuração do Flow Analysis consiste nas seguintes tarefas:



Um administrador do sistema com o conhecimento do Windows Server 2008 e direitos administrativos nos hosts executa essas etapas de configuração:

1. Abrir a porta 9995 ao tráfego UDP no sistema do coletor do Flow Analysis
2. Ativar o NetFlow (ou outro protocolo de monitoramento de fluxo) na interface do dispositivo de rede como o desejado (um administrador de rede com o acesso administrativo a esses dispositivos pode ser necessário para executar esta etapa)
3. Configurar o probe do Flow Analysis
4. Configurar o coletor do Flow Analysis
5. Configurar relatórios.

Abrir a porta 9995

Abrir a porta 9995 ao tráfego UDP no sistema do coletor. Confirmar se o tráfego UDP pode passar entre seus dispositivos de rede e o host do coletor que está usando esta porta.

Ativar o NetFlow em dispositivos de rede

Para ativar o NetFlow em roteadores compatíveis com o NetFlow, execute as seguintes etapas em cada roteador com suporte para versões 5, 7 e 9 do NetFlow.

Observação: antes de começar, colete as informações a seguir para cada roteador que desejar monitorar:

- Endereço de origem
- Sequência de caracteres da comunidade de leitura SNMP
- Versão do NetFlow (se aplicável)

Protocolos de fluxo compatíveis:

- NetFlow v5, v7 e v9
- sFlow versão 5
- IPFIX, Jflow, cFlow e NetStream padrões e em conformidade com os padrões para o NetFlow v5, v7 ou v9

Siga estas etapas:

1. Salve uma cópia de backup das configurações atuais para um servidor TFTP (Trivial File Transfer Protocol - Protocolo de transferência de arquivo simples) ou para a área de trabalho.
2. Execute o comando **copy run start** ou **wr mem** antes de fazer quaisquer alterações nos roteadores que deseja monitorar.

   A execução deste comando ajuda a garantir que todas as configurações atuais serão salvas na memória estática caso o roteador bloqueie ou reinicie.
3. Configure a exportação do NetFlow inserindo os seguintes comandos IOS na ordem mostrada:

   ```
   ip flow-export version <version_number>
   ip flow-export source <interface>
   ip flow-export destination <IP address of the installation system>
   9995
   ip flow-cache timeout active 1
   ```

   Observação: para o segundo comando na série, o endereço IP da interface de origem pode ser alterado. A Cisco recomenda que você configure uma interface de origem loopback para usar.

4. Para cada interface lógica, vá para a interface e digite:
   `ip route-cache flow`

   ou
   `ip flow ingress (para versões mais recentes do IOS)`

5. Configure a persistência do índice em cada roteador usando o seguinte comando:
   `config# snmp-server ifindex persist`

   Observação: os Roteadores da Cisco das famílias das séries 7200, 7500 e 12000 GSR suportam a persistência de índice.

6. Verifique se você possui um Sup II ou mecanismo de supervisão superior, se você usar os switches Catalyst 6500 e 7600.

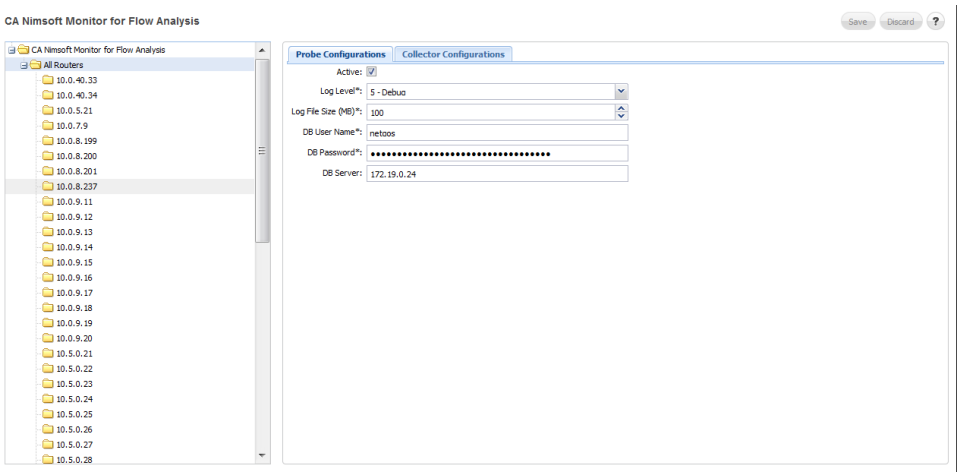
   Observação: para outros comandos de switch Catalyst 6500 e 7600, consulte a documentação de comandos do NetFlow da Cisco.

Verifique se os dados do fluxo estão sendo recebidos

No sistema do Coletor (onde o componente do software do Banco de dados do Flow Analysis está instalado), acesse o diretório D:\NETQOS\Netflow\datafiles\Harvester\Work. Deve haver muitos arquivos neste diretório chamado <numeric_value>-9995.tbn.inc. Pode haver mais arquivos com o mesmo esquema de nomenclatura com uma extensão de arquivo .tmp. Se você visualizar arquivos <numeric_value> -9995.tbn.inc que são maiores que 0 KB, isso indica que o fluxo de dados está sendo recebido.

Abrindo a interface gráfica do usuário (GUI) de configuração

Clique no botão **Configurar** na parte superior direita da GUI do Flow Analysis no UMP para abrir a interface gráfica de configuração em uma janela separada:

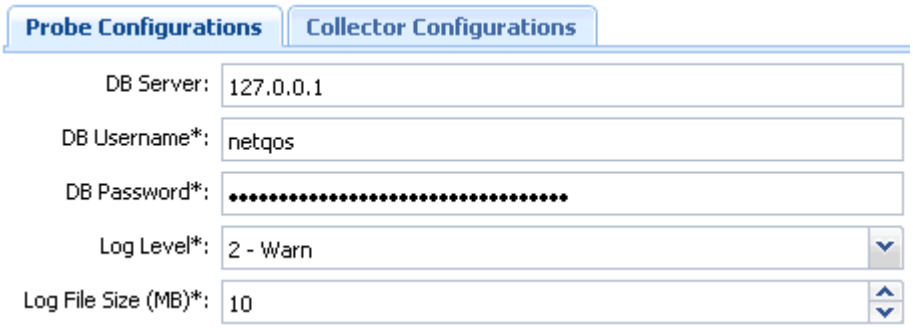


Quando a interface do usuário de configuração é iniciada pela primeira vez, não existe nenhum dado no quadro do lado esquerdo a ser exibido até que um coletor esteja ativado. Com um Coletor ativado, uma hierarquia de dispositivos de rede é exibida.

No quadro direito, há duas guias, **Configurações de probe** e **Configurações do coletor**, as quais controlam as configurações para o probe e coletor do Flow Analysis, respectivamente.

Configurar o probe do Flow Analysis

A guia Configurações do probe na interface gráfica de usuário de configuração do Flow Analysis permite definir e alterar estes atributos:



Campo	Descrição
DB Server	Endereço IP do Banco de dados do Flow Analysis.
Nome de usuário de DB	Nome do usuário do Banco de dados do Flow Analysis. O padrão é **netqos**.
Senha DB	Senha para o Nome de usuário do banco de dados. O padrão é **netqos**.
Nível de log	Nível de detalhe do arquivo de log. O nível mais detalhado é o 5, Rastreamento.
Tamanho do arquivo de log (MB)	O tamanho máximo, em megabytes, para o arquivo de log.

Configurar o coletor do Flow Analysis

Os atributos a seguir para o probe do Flow Analysis são definidos usando a guia **Configurações do Coletor** a partir da interface gráfica do usuário de configuração do Flow Analysis.

Siga estas etapas:

1. Verifique se o Usuário do administrador do Windows e senha inseridos durante a instalação foram armazenados com êxito no banco de dados.

   Em geral, isso é processado durante a instalação, mas ocasionalmente ocorre um erro.

   Importante: Se o Usuário administrador do Windows e senha (que são os mesmos do Nome de usuário do administrador do DSA e Senha do administrador do DSA na guia de configurações do Coletor) não estiverem armazenados no banco de dados, o Flow Analysis não terá acesso ao compartilhamento do Coletor no sistema do Coletor e nenhum dado poderá ser coletado.

   Execute as etapas a seguir para confirmar se o nome de usuário e a senha foram definidos:

   a. Abra o seguinte arquivo de log para visualização:

      C:\tmp\ia\NimsoftFlowAnalysis.log

   b. Procure pelo seguinte texto:

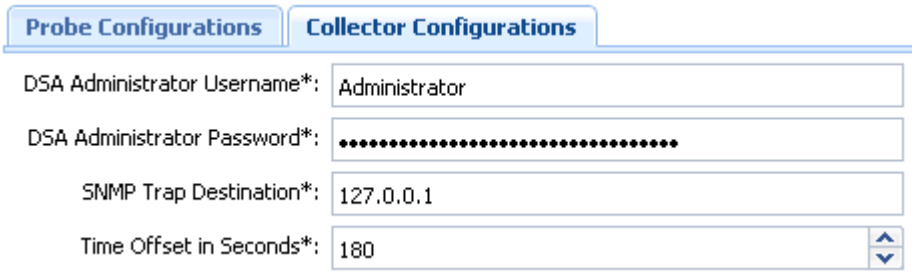
      `SUCCESS: Flow Analysis Collector credentials configured.`

   Se o texto estiver presente, o Usuário administrador do Windows e a senha inseridos durante a instalação foram armazenados com êxito no banco de dados.

   Se o texto NÃO estiver presente, insira as credenciais nos campos de **Nome de usuário do administrador do DSA** e **Senha do administrador do DSA** na guia de **Configurações do Coletor**.

2. Digite o **Destino de interceptação SNMP**.

3. Reinicialize o sistema do coletor para instanciar essas alterações.



Observação: as alterações feitas aqui são aplicadas para o coletor que está atualmente selecionado na barra superior do menu da interface de usuário de relatórios do Flow Analysis.

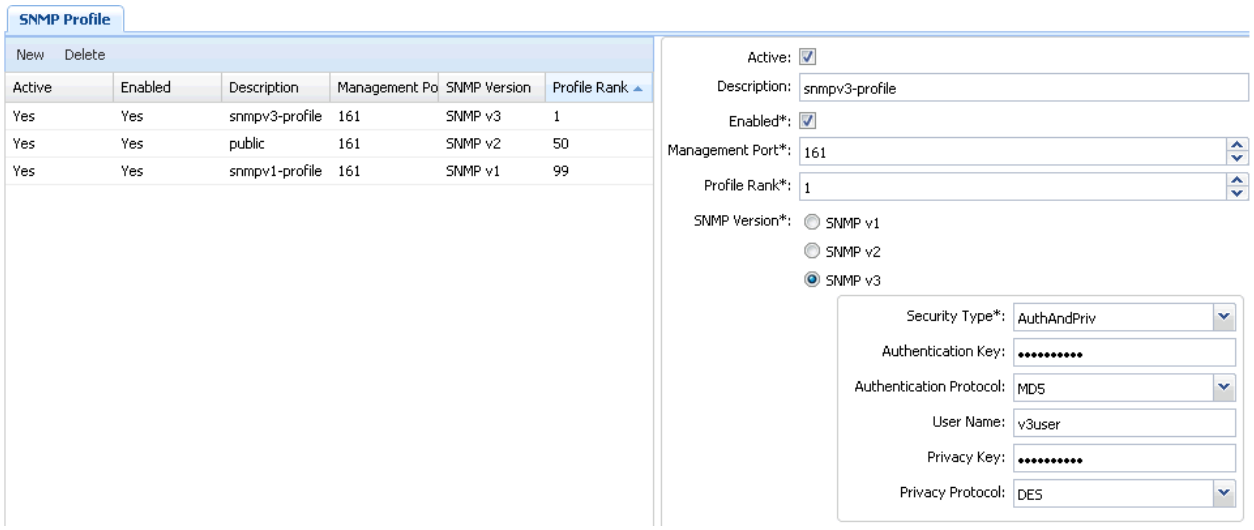
Campo	Tipo	Descrição
Nome de usuário do administrador DSA	Endereço IP \ sequência de caracteres	Um usuário do Windows que tenha privilégios administrativos no sistema do Coletor. Geralmente, isso é definido durante a instalação no Coletor. Se você não souber o nome do administrador do DSA, verifique com o administrador do servidor. Exemplo: 127.0.0.1\administrator (o padrão)
Senha do administrador do DSA	sequência de caracteres	Senha do administrador do DSA.
Destino de interceptação do SNMP	Endereço IP	Endereço IP do robô que controla os probes flow e snmptd no sistema do Coletor.
Diferença de tempo em segundos	inteiro> 0	Número de segundos a ser subtraído do horário de término de consultas ao banco de dados. O padrão é 180 (3 minutos). Por exemplo, ao solicitar um relatório dos últimos 15 minutos, às 10h, o intervalo de consulta diminui três minutos, das 9h42min às 9h57min. Isso retorna o intervalo de relatório de dados de 15 minutos que se encerra nesse período, os dados entre 9h30min e 9h45min. Se o banco de dados for consultado por dados até o minuto atual, os dados poderão não estar disponíveis e nenhum dado será retornado. A diferença de três minutos evita problemas causados pela latência do banco de dados. Se você solicitar dados para os últimos 15 minutos às 10h03min, os dados entre 9h45min às 10h serão exibidos. Em geral, quanto mais rápida o sistema do coletor for, menor esse intervalo pode ser, e vice-versa. **Importante:** NÃO altere esse valor do padrão, a menos que seja instruído a fazê-lo pelo Suporte técnico do Nimsoft da CA.

Mais informações:

Sem dados exibidos em relatórios (Tempo de atraso nos dados relatados) (na página 37)

Configurar perfis de SNMP

Clicar em **Todos os roteadores** na árvore exibirá a tela **Perfil de SNMP** no quadro direito:



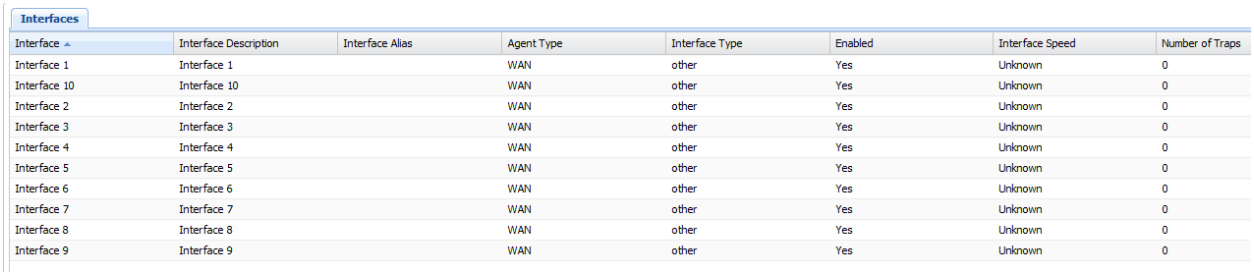
Clicar em **Novo** no Perfil de SNMP, ou clicar em um perfil existente, exibirá os campos de configuração do **Perfil de SNMP** à direita.

Observação: quando você criar ou editar perfis de SNMP, os perfis poderão não responder imediatamente. Poderá demorar até uma hora para que as alterações sejam refletidas na guia **Respondendo a perfis de SNMP**.

Campo	**Descrição**
Ativo	Independentemente de o perfil ser aplicado ao dispositivo selecionado. O padrão é **Ativo**.
Descrição	Digite o texto para descrever o perfil.
Ativado	Independentemente de o perfil ser usado ao tentar se comunicar com o dispositivo selecionado. O padrão é **Ativo**.
Porta de gerenciamento	Porta para o Coletor do Flow Analysis usar para se comunicar com o roteador. O padrão é **161**.
Classificação do perfil	Ordem na qual um perfil é tentado/correspondido em relação a um roteador.
Versão do SNMP	Definir a **Sequência de caracteres da comunidade** para SNMP v1 e v2
	Para SNMP v3, escolha o **Tipo de segurança**. Dependendo do **Tipo de segurança** escolhido, alguns campos podem ser desativados. Digite as informações nos campos ativos. Se você não souber as informações, entre em contato com seu administrador de SNMP.

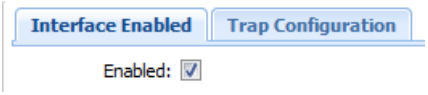
Configurar Interfaces

Clicar em um dispositivo de rede listado no quadro esquerdo exibe as **Interfaces** que estão disponíveis no dispositivo de rede selecionado:



Interface	Interface Description	Interface Alias	Agent Type	Interface Type	Enabled	Interface Speed	Number of Traps
Interface 1	Interface 1		WAN	other	Yes	Unknown	0
Interface 10	Interface 10		WAN	other	Yes	Unknown	0
Interface 2	Interface 2		WAN	other	Yes	Unknown	0
Interface 3	Interface 3		WAN	other	Yes	Unknown	0
Interface 4	Interface 4		WAN	other	Yes	Unknown	0
Interface 5	Interface 5		WAN	other	Yes	Unknown	0
Interface 6	Interface 6		WAN	other	Yes	Unknown	0
Interface 7	Interface 7		WAN	other	Yes	Unknown	0
Interface 8	Interface 8		WAN	other	Yes	Unknown	0
Interface 9	Interface 9		WAN	other	Yes	Unknown	0

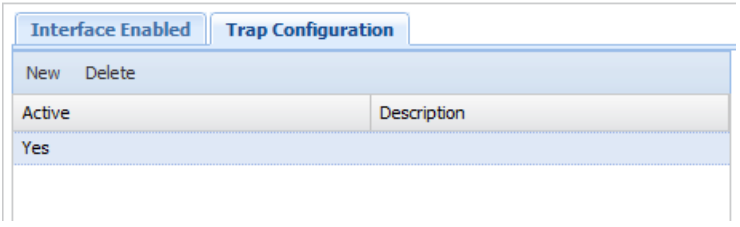
Clicar em uma interface exibe a interface do usuário de configuração da **Interface ativa** abaixo:



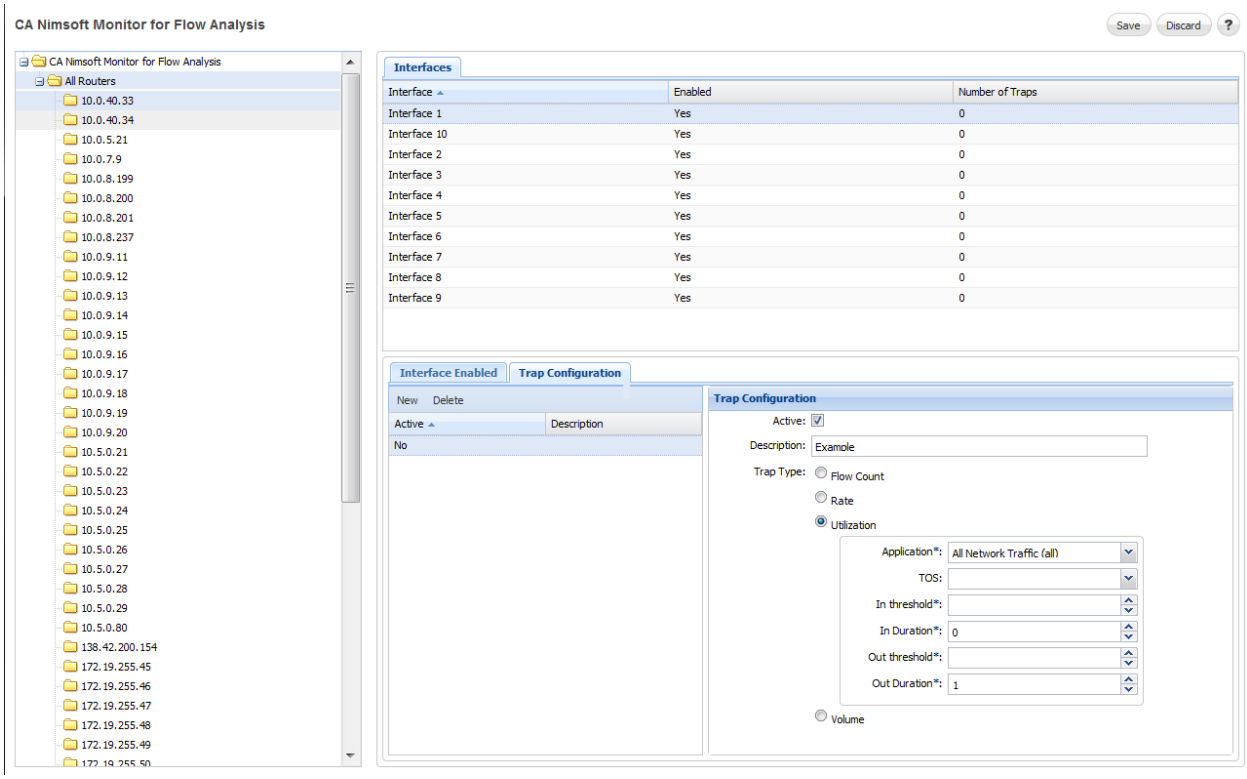
Atributo	Tipo	Observações
Ativado	boolean	se a interface está sendo monitorada ou não para dados do NetFlow; default=enabled

Configurar interceptações

Clicar em **Configuração de Interceptação** exibe uma lista de interceptações definidas na interface específica do dispositivo de rede selecionado:



Clicar em uma configuração de interceptação na lista exibe a GUI de **Configuração de interceptação** à direita:

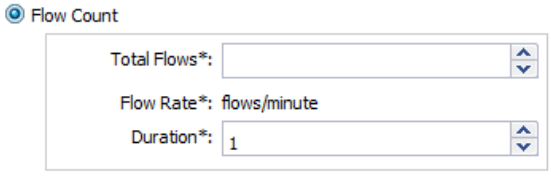


Todos os tipos de interceptação compartilham dois atributos -- Ativo e Descrição.

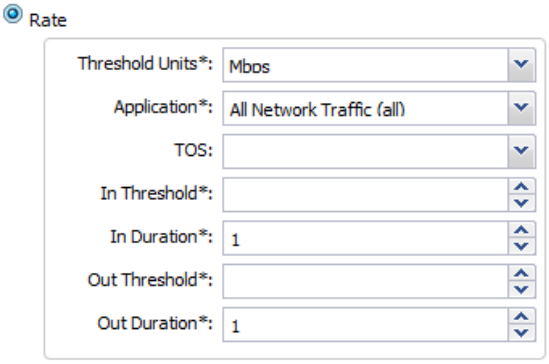
Atributo	Tipo	Observações
Ativo	boolean	se uma interceptação SNMP for emitida ou não para a configuração especificada e interface atribuída; padrão=ativo
Descrição	sequência de caracteres	

Cada tipo de interceptação oferece atributos de configuração adicionais específicos aos seus objetivos:

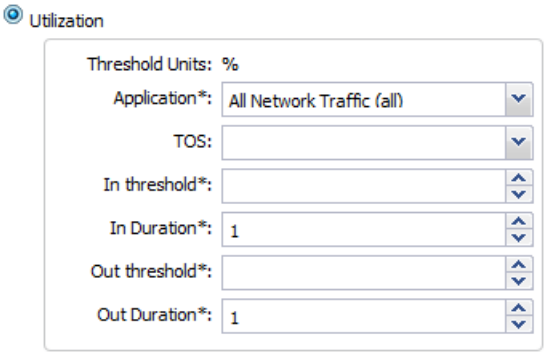
Contagem de fluxo



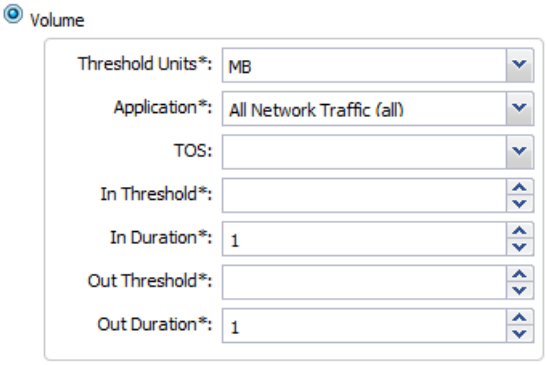
Taxa



Utilização



Volume



Configurar relatórios

Depois que as etapas de configuração anteriores são realizadas, você estará pronto para visualizar os relatórios do Flow Analysis.

Consulte a seção sobre Relatórios (na página 27) para obter uma descrição sobre como configurar e usar os relatórios do Flow Analysis e as opções que estão disponíveis.

Capítulo 3: Relatórios

Esta seção contém os seguintes tópicos:

Relatórios de dados do Flow Analysis

A interface web do Flow Analysis oferece uma visão integrada dos aplicativos N principais, os hosts e interfaces de dispositivos da rede. Esta seção descreve os tipos de relatórios e as opções que estão disponíveis.

O Flow Analysis oferece uma exibição multidimensional do fluxo de dados recebidos da infraestrutura da sua rede. É possível passar os dados para responder a esses e outros tipos de perguntas:

- Quem conversou com quem? Quando? (Otimização da alocação da largura de banda e economia de custos ou detectar o tráfego mal-intencionado)
- Qual protocolo é mais intensamente usado? (Ofertas de classe de otimização de serviços)
- Onde está o maior volume de tráfego de rede? (Otimizar as configurações de VPN e alocação de largura de banda; solucionar problemas de alterações repentinas no uso)
- Que tipo de serviço (por exemplo, platina, ouro ou prata) está sendo afetado?

Usar a geração de relatórios de fluxo de dados juntamente com os relatórios de dados do QoS no UMP, é possível visualizar seu ambiente de serviço de TI a partir de uma perspectiva especifica a um dispositivo, serviço ou aplicativo.

Noções básicas sobre intervalos de relatórios de dados

A maioria dos dados do probe Flow Analysis são armazenados como dados agregados para intervalos de 15 minutos. Os dados para cada intervalo de 15 minutos, encerrado no intervalo de tempo especificado, serão incluídos no relatório. Se, por exemplo, às 12h05min, você solicitar um relatório dos principais 10 para os últimos 15 minutos, os dados agregados para o intervalo entre 11h45min às 12h serão exibidos. Se, às 12h05min, você solicitar dados para a última hora, verá os dados para o intervalo entre 11h e 12h.

A exceção para isso é quando você fizer o detalhamento a um relatório para uma interface. Para interfaces, os dados para as últimas 24 horas são armazenados em intervalos de um minuto; dados anteriores a 24 horas são armazenados em intervalos de 15 minutos.

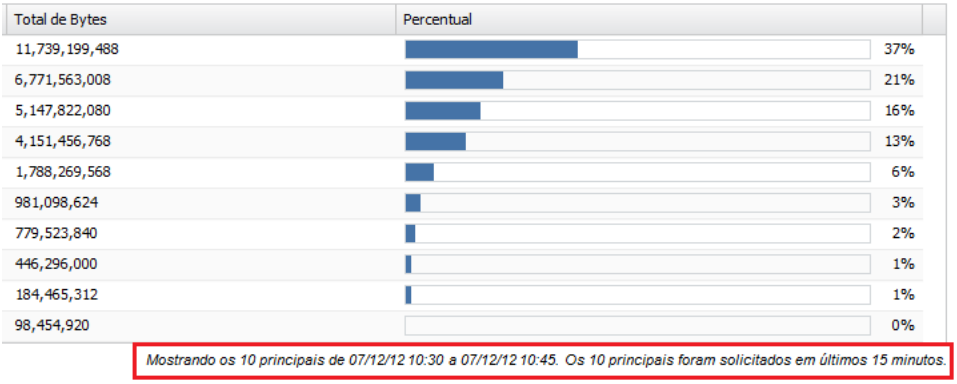
Os dados de um minuto ajudam na solução de problemas, quando você necessitar de dados detalhados e atuais para uma interface. Ao clicar no nome de uma interface no gráfico de Interfaces principais gráfico na janela principal, o relatório da interface será exibido mostrando dados de intervalos de 1 minuto, se possível. Há casos em que são mostrados dados de 15 minutos para relatório de detalhamento de interface:

- Se o intervalo de relatório solicitado ultrapassa 24 horas. Os dados de um minuto são armazenadas somente para as últimas 24 horas. Se dados anteriores a 24 horas forem solicitados, somente intervalos de 15 minutos estarão disponíveis.
- Se o intervalo de relatório solicitado for superior a cinco horas. Para evitar problemas de desempenho devido ao processamento de grandes quantidades de dados, os dados de 15 minutos serão exibidos para intervalos de relatório superiores a cinco horas.

Dados para hosts principais e aplicativos principais serão armazenados somente em intervalos de 15 minutos, incluindo para relatórios de detalhamento.

Por que o intervalo exibido é diferente do intervalo solicitado?

A legenda abaixo de cada gráfico indica o intervalo dos dados exibidos e o intervalo de dados solicitado. Às vezes, o intervalo exibido será ligeiramente diferente do intervalo de dados solicitado. Por exemplo, na imagem abaixo, os dados dos últimos 15 minutos foram solicitados às 10h52min e os dados entre 10h30min e 10h45min foram exibidos.



Isso ocorre porque os dados do Flow Analysis são armazenados em fragmentos de 15 minutos. Ao solicitar dados dos últimos 15 minutos, os dados para o fragmento que termina dentro dos últimos 15 minutos serão exibidos. Portanto, quando às 10h52min, você solicitar dados dos últimos 15 minutos (das 10h37min às 10h52min), o fragmento encerrando nesse intervalo consistirá nos dados para o intervalo entre 10h30min e 10h45min.

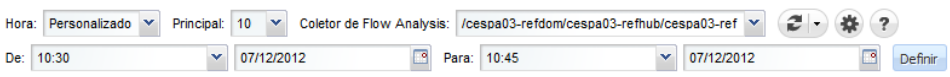
Além disso, há uma pequena demora (até 3 minutos) enquanto os dados são armazenados no banco de dados. Portanto, se às 11h você solicitar os dados dos últimos 15 minutos, poderá ver os dados para o intervalo entre 10h30min e 10h45min. Portanto, se às 11h03min você solicitar os dados dos últimos 15 minutos, poderá ver os dados para o intervalo entre 10h45min e 11h.

Observação: o atraso não ocorre ao visualizar dados de um minuto nos relatórios de detalhamento de interface.

Elementos comuns

Os seguintes elementos de GUI estão disponíveis em todos os relatórios do porlet do Flow Analysis:

Elementos da barra superior



1. Tempo -- o intervalo de tempo no qual os dados exibidos são coletados (últimos 14 minutos (padrão), última hora, últimas 4 horas, último dia, última semana, Personalizar)
2. Principais -- número de interfaces/hosts/aplicativos mostrados nos relatórios dos N principais (5, 10 (padrão), 15, 20, 25)
3. Coletor do Flow Analysis -- o coletor que está fornecendo dados para os relatórios; também conhecido como o Probe do Flow Analysis
4. Botão Atualizar -- consulta o banco de dados para os últimos intervalos de dados. Pode ser definido como: manual e atualização automática (intervalos de 1, 5, 10 e 15 minutos)
5. Botão Configurar -- abre o painel de Configuração
6. Botão Ajuda -- exibe a ajuda online
7. De, Para e Definir -- visível somente se você escolher Personalizar para o campo Horário. Esses campos permitem selecionar um intervalo de tempo para a exibição de dados. Digite informações de data e hora nos campos De e Para; em seguida, clique em Definir. O intervalo de tempo deve ser nos últimos 31 dias.

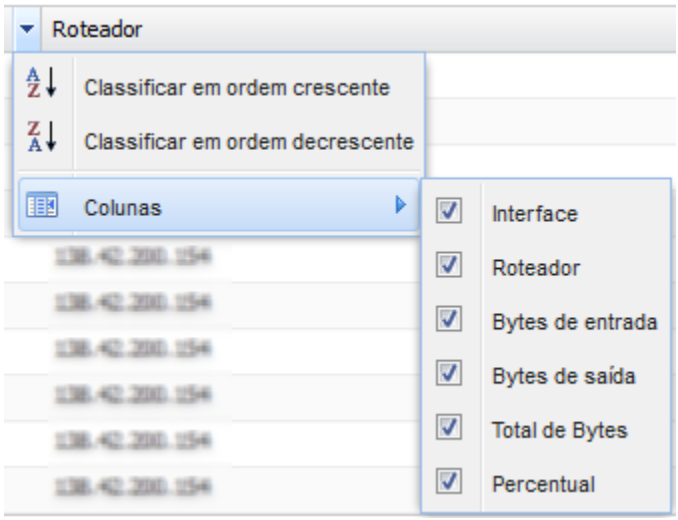
Opções de gráfico

1. Gráfico de coluna
2. Gráfico de barras
3. Gráfico de linhas
4. Exportar para o CSV. 

Clique no ícone e digite um local de salvamento. Os dados exibidos no relatório é o que é salvo.

Opções de exibição da coluna

Clicar em um cabeçalho de coluna alterna os dados abaixo na ordem de classificação crescente ou decrescente. É possível ocultar ou exibir colunas usando as caixas de seleção.



Arrastar colunas

É possível arrastar colunas inteiras em uma ordem de preferência. Este reordenamento de coluna não é persistente se você atualizar ou fechar o navegador.

Detalhar links

Clique nos links em azul para as interfaces, hosts, conversas e outros itens. Cada visualização no UMP é um "URL avançado" que, se copiado e colado em outra guia ou janela do navegador, exibirá o mesmo relatório/página da web, com dados atualizados para o intervalo de tempo mais recente.

	Host	Bytes de entrada	Bytes de saída
1	[redacted]	34,282,020	2,732,244,224

Exibir dicas de ferramentas

Exibe informações detalhadas para alguns itens em exibições de relatório ao posicionar o cursor sobre o item. Quando você passa o cursor sobre o gráfico de barras de dados você obtém uma dica de ferramenta e os dados correspondentes na tabela são realçados. Inversamente, ao passar o mouse sobre uma linha de dados em uma tabela destaca o gráfico de barra correspondente.

Sequência de caracteres de informação

Abaixo de cada relatório gráfico na parte inferior direita existe uma legenda que fornece detalhes sobre os dados exibidos no relatório.

Página principal do Flow Analysis

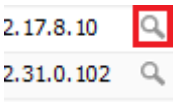
A janela principal do Flow Analysis exibe os N principais dados para fluxos de dados entre:

- Interfaces principais
- Hosts principais
- Aplicativos principais (protocolos)

Clicar em um nome de interface no gráfico de interfaces principais exibirá um relatório de detalhamento sobre as N principais conversas/hosts/aplicativos a partir da perspectiva daquela interface.

Da mesma forma, clicar em um nome de host ou aplicativo em seus respectivos gráficos detalhará o host ou aplicativo e fornecerá informações adicionais.

Se um ícone de lupa aparecer ao lado do nome de um dispositivo, será possível clicar no ícone para pesquisar pelo dispositivo no Unified Service Manager (dependendo do dispositivo, nem todas as pesquisas fornecerão informações adicionais).

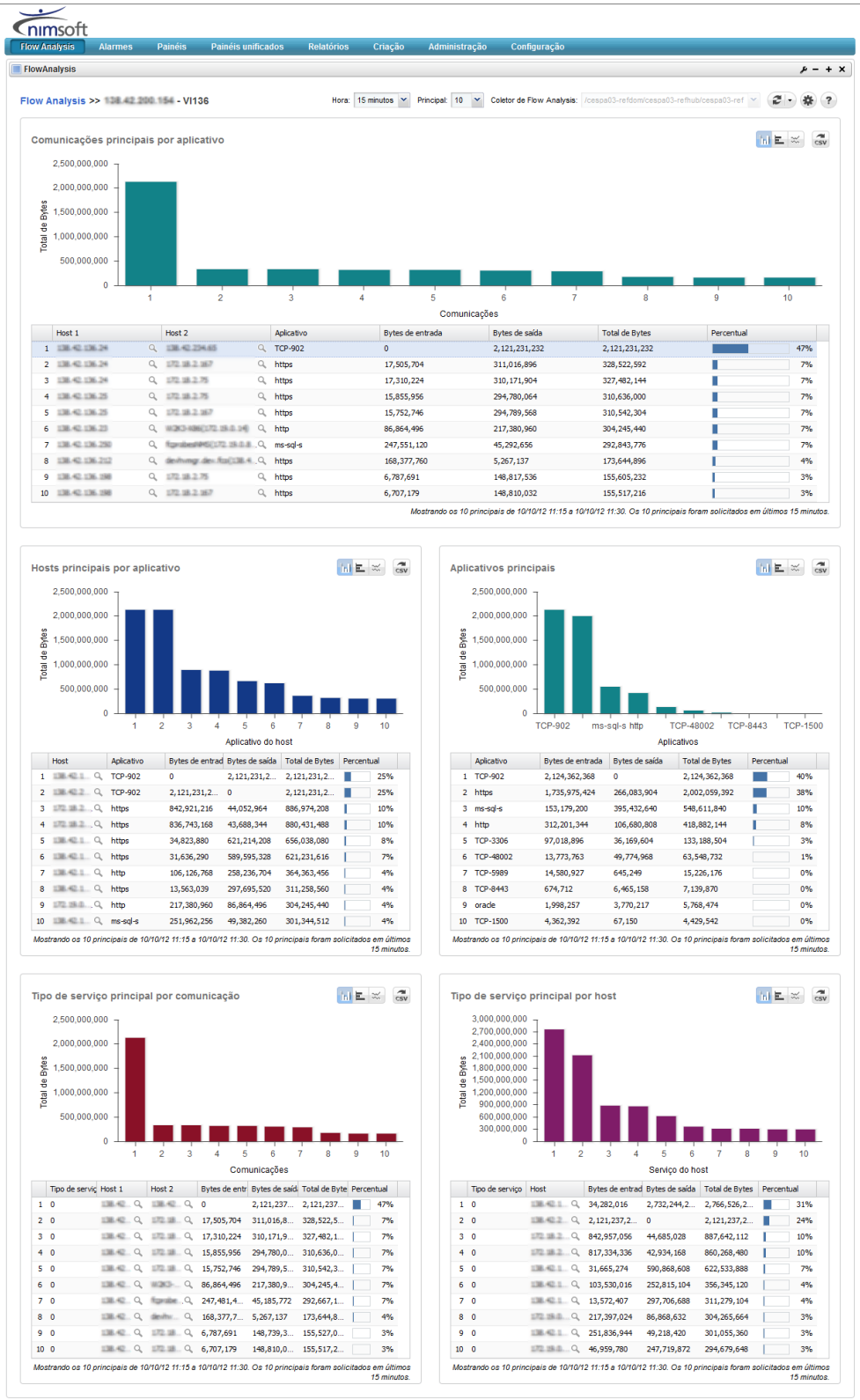


Interfaces

No relatório principal, fazer uma busca detalhada em uma interface mostra o tráfego que está fluindo pela interface do dispositivo de rede selecionado. Essas informações são úteis para otimizar as configurações de VPN e alocação de largura de banda, ajuste fino das opções de serviço, ou solução de problemas de mudanças inesperadas no uso. Elas podem ser usadas para otimizar alocações de largura de banda ou para detectar o tráfego mal-intencionado.

Estes relatórios são exibidos:

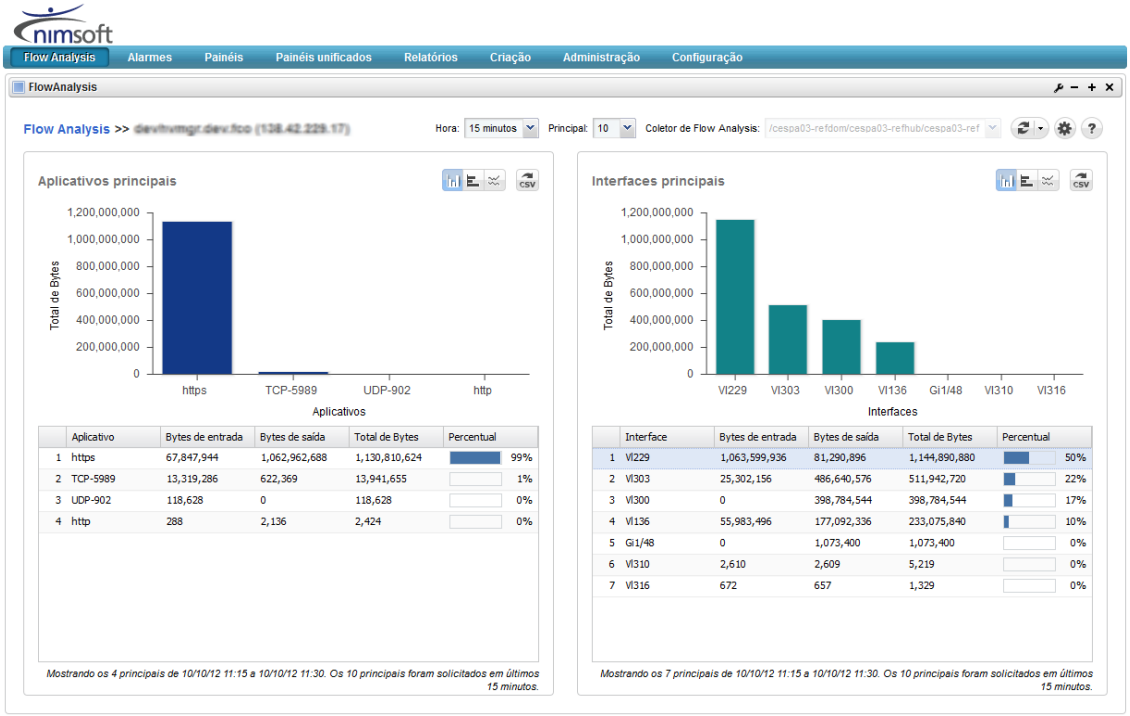
- Principais conversas por aplicativo
- Principais hosts por aplicativo
- Principais aplicativos
- Principais tipos de serviço por conversação
- Principais tipos de serviço por host


nimsoft
Flow Analysis
Alarmes
Painéis
Painéis unificados
Relatórios
Criação
Administração
Configuração
FlowAnalysis
Flow Analysis >> 138.42.200.154 - VI136
Hora: 15 minutos
Principal: 10
Coletor de Flow Analysis:
Comunicações principais por aplicativo
Total de Bytes
Comunicações
Host 1 | Host 2 | Aplicativo | Bytes de entrada | Bytes de saída | Total de Bytes | Percentual
1 | TCP-902 | 0 | 2,121,231,232 | 2,121,231,232 | 47%
2 | https | 17,505,704 | 311,016,896 | 328,522,592 | 7%
3 | https | 17,310,224 | 310,171,904 | 327,482,144 | 7%
4 | https | 15,855,956 | 294,780,064 | 310,636,000 | 7%
5 | https | 15,752,746 | 294,789,568 | 310,542,304 | 7%
6 | http | 86,864,496 | 217,380,960 | 304,245,440 | 7%
7 | ms-sql-s | 247,551,120 | 45,292,656 | 292,843,776 | 7%
8 | https | 168,377,760 | 5,267,137 | 173,644,896 | 4%
9 | https | 6,787,691 | 148,817,536 | 155,605,232 | 3%
10 | https | 6,707,179 | 148,810,032 | 155,517,216 | 3%
Mostrando os 10 principais de 10/10/12 11:15 a 10/10/12 11:30. Os 10 principais foram solicitados em últimos 15 minutos.
Hosts principais por aplicativo
Total de Bytes
Aplicativo do host
Host | Aplicativo | Bytes de entrad | Bytes de saída | Total de Bytes | Percentual
1 | TCP-902 | 0 | 2,121,231,2... | 2,121,231,2... | 25%
2 | TCP-902 | 2,121,231,2... | 0 | 2,121,231,2... | 25%
3 | https | 842,921,216 | 44,052,964 | 886,974,208 | 10%
4 | https | 836,743,168 | 43,688,344 | 880,431,488 | 10%
5 | https | 34,823,880 | 621,214,208 | 656,038,080 | 8%
6 | https | 31,636,290 | 589,595,328 | 621,231,616 | 7%
7 | http | 106,126,768 | 258,236,704 | 364,363,456 | 4%
8 | https | 13,563,039 | 297,695,520 | 311,258,560 | 4%
9 | http | 217,380,960 | 86,864,496 | 304,245,440 | 4%
10 | ms-sql-s | 251,962,256 | 49,382,260 | 301,344,512 | 4%
Mostrando os 10 principais de 10/10/12 11:15 a 10/10/12 11:30. Os 10 principais foram solicitados em últimos 15 minutos.
Aplicativos principais
Total de Bytes
TCP-902
ms-sql-s
http
TCP-48002
TCP-8443
TCP-1500
Aplicativos
Aplicativo | Bytes de entrada | Bytes de saída | Total de Bytes | Percentual
1 | TCP-902 | 2,124,362,368 | 0 | 2,124,362,368 | 40%
2 | https | 1,735,975,424 | 266,083,904 | 2,002,059,392 | 38%
3 | ms-sql-s | 153,179,200 | 395,432,640 | 548,611,840 | 10%
4 | http | 312,201,344 | 106,680,808 | 418,882,144 | 8%
5 | TCP-3306 | 97,018,896 | 36,169,604 | 133,188,504 | 3%
6 | TCP-48002 | 13,773,763 | 49,774,968 | 63,548,732 | 1%
7 | TCP-5989 | 14,580,927 | 645,249 | 15,226,176 | 0%
8 | TCP-8443 | 674,712 | 6,465,158 | 7,139,870 | 0%
9 | oracle | 1,998,257 | 3,770,217 | 5,768,474 | 0%
10 | TCP-1500 | 4,362,392 | 67,150 | 4,429,542 | 0%
Mostrando os 10 principais de 10/10/12 11:15 a 10/10/12 11:30. Os 10 principais foram solicitados em últimos 15 minutos.
Tipo de serviço principal por comunicação
Total de Bytes
Comunicações
Tipo de serviç | Host 1 | Host 2 | Bytes de entr | Bytes de saíd | Total de Byte | Percentual
1 | 0 | 0 | 2,121,237... | 2,121,237... | 47%
2 | 0 | 17,505,704 | 311,016,8... | 328,522,5... | 7%
3 | 0 | 17,310,224 | 310,171,9... | 327,482,1... | 7%
4 | 0 | 15,855,956 | 294,780,0... | 310,636,0... | 7%
5 | 0 | 15,752,746 | 294,789,5... | 310,542,3... | 7%
6 | 0 | 86,864,496 | 217,380,9... | 304,245,4... | 7%
7 | 0 | 247,481,4... | 45,185,772 | 292,667,1... | 7%
8 | 0 | 168,377,7... | 5,267,137 | 173,644,8... | 4%
9 | 0 | 6,787,691 | 148,739,3... | 155,527,0... | 3%
10 | 0 | 6,707,179 | 148,810,0... | 155,517,2... | 3%
Mostrando os 10 principais de 10/10/12 11:15 a 10/10/12 11:30. Os 10 principais foram solicitados em últimos 15 minutos.
Tipo de serviço principal por host
Total de Bytes
Serviço do host
Tipo de serviço | Host | Bytes de entrad | Bytes de saída | Total de Bytes | Percentual
1 | 0 | 34,282,016 | 2,732,244,2... | 2,766,526,2... | 31%
2 | 0 | 2,121,237,2... | 0 | 2,121,237,2... | 24%
3 | 0 | 842,957,056 | 44,685,028 | 887,642,112 | 10%
4 | 0 | 817,334,336 | 42,934,168 | 860,268,480 | 10%
5 | 0 | 31,665,274 | 590,868,608 | 622,533,888 | 7%
6 | 0 | 103,530,016 | 252,815,104 | 356,345,120 | 4%
7 | 0 | 13,572,407 | 297,706,688 | 311,279,104 | 4%
8 | 0 | 217,397,024 | 86,868,632 | 304,265,664 | 3%
9 | 0 | 251,836,944 | 49,218,420 | 301,055,360 | 3%
10 | 0 | 46,959,780 | 247,719,872 | 294,679,648 | 3%
Mostrando os 10 principais de 10/10/12 11:15 a 10/10/12 11:30. Os 10 principais foram solicitados em últimos 15 minutos.

Hosts

Na exibição principal, fazer uma busca detalhada em um host fornece dois relatórios sobre o tráfego visto naquele host:

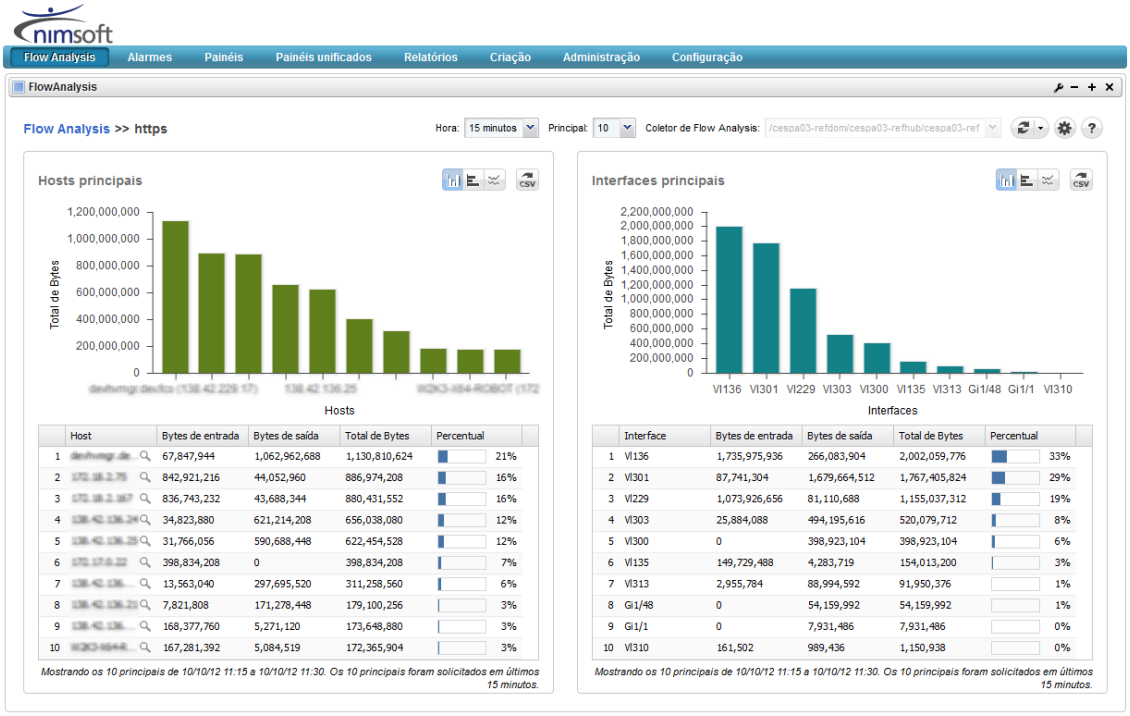
- Aplicativos principais
- Interfaces principais



Aplicativos

Fazer uma busca detalhada em um aplicativo a partir da tela principal exibe, dependendo do protocolo, até dois relatórios detalhados:

- Hosts principais
- Interfaces principais



Apêndice A: Solução de problemas

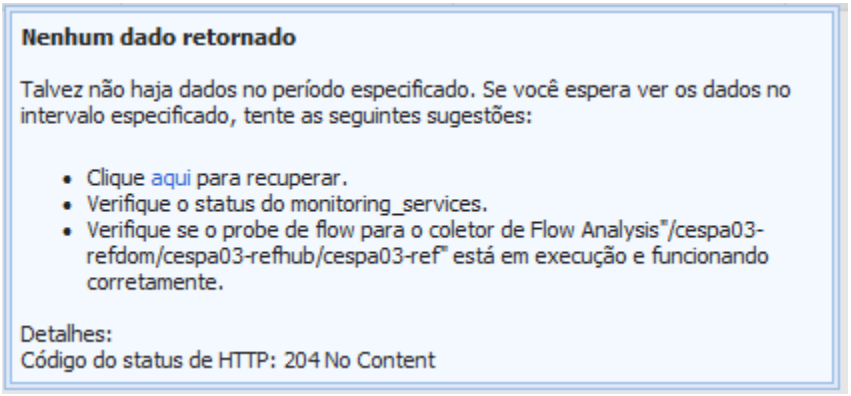
Esta seção contém os seguintes tópicos:

Sem dados exibidos em relatórios (Tempo de atraso nos dados relatados)

Válido em todas as plataformas

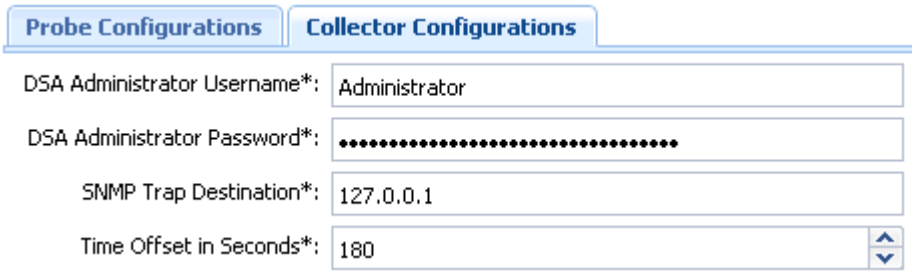
Sintoma:

Continuo vendo esta mensagem de erro



Solução:

Aumente a configuração de **Diferença de horário** na guia de Configurações do Coletor.



A configuração de **Diferença de horário em segundos** para um valor superior pode ser necessária para sistemas do Coletor do Flow Analysis lentos. Não defina esse valor como um valor superior a 500 ou haverá um atraso significativo ao exibir relatórios.

Mais informações:

Configurar o coletor do Flow Analysis (na página 20)

O portlet FlowAnalysis exibe uma mensagem de erro de comunicação

Válido em todas as plataformas

Sintoma:

O portlet FlowAnalysis exibe uma mensagem de erro de comunicação:

```
Falha de comunicação

Ocorreu um erro ao tentar recuperar Coletores do Flow Analysis. O navegador perdeu
temporariamente a comunicação com o servidor do UMP. Os erros de comunicação do
servidor podem ser causados por uma interrupção na rede, uma rede lenta ou por
o servidor estar inoperante. Se o erro persistir, tente uma das seguintes
sugestões:

    Clique aqui para tentar novamente.
    Tente efetuar logoff e efetuar logon novamente.
    Verifique o status da rede, do ump_monitoring_services e do ambiente do UMP.

Detalhes:
Código de status HTTP: 404 Não Encontrado
```

Solução:

Arraste o pacote do probe ump_monitoring_services v1.03 do arquivo local do Nimsoft para o ícone do robô do sistema UMP usando o Infrastructure Manager. O probe ump_monitoring_services, exigido pelo probe ump_flow, é instalado automaticamente ao arrastar o portlet ump_flow e ao soltá-lo no ícone do robô do sistema UMP. Mas em algumas instalações, um probe ump_monitoring_services incompatível mais recente, Serviços de monitoramento (Edição Host de serviço) v1.2, é implantado no controlador/robô.

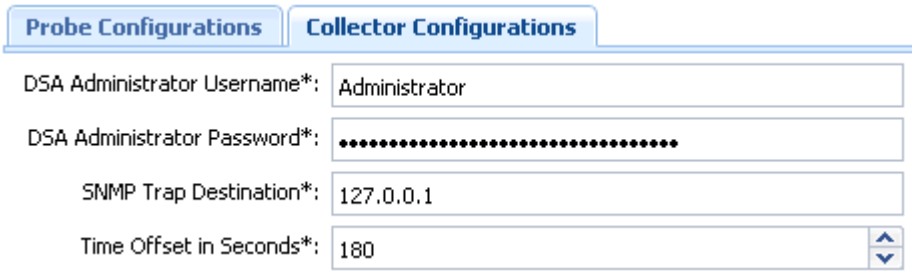
O Flow Analysis interrompe a coleta após 15 minutos

Sintoma:

O probe do Flow Analysis pareceu funcionar por 15 minutos e então interrompeu a coleta de dados.

Solução:

As credenciais do Administrador do Windows (DSA) para o sistema do Coletor do Flow Analysis não estão corretas. Insira as credenciais nos campos de **Nome de usuário do administrador do DSA** e **Senha do administrador do DSA** da guia de **Configurações do Coletor** na janela de Configuração do probe.



O nome de usuário inserido deve ter privilégios de administrador no sistema do Coletor do Flow Analysis.

Links para USM não tem função

Válido em todas as plataformas

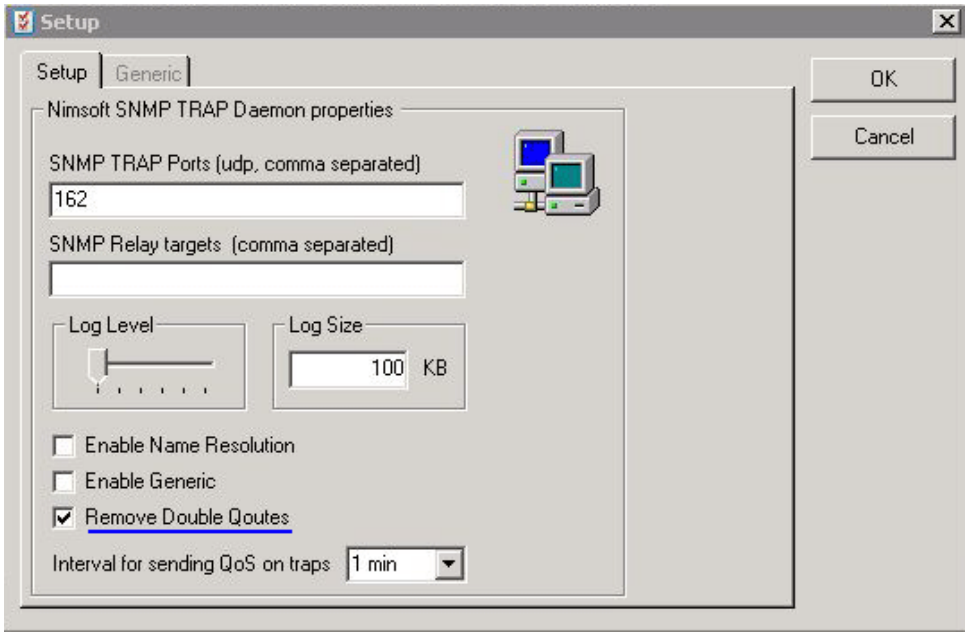
Sintoma:

Quando clico no ícone de lupa para "pesquisa do USM" na interface gráfica do usuário do Flow Analysis, o sistema mostra a mensagem "Nenhuma métrica disponível". Isso ocorre para todos os dispositivos que pesquiso no USM.

Solução:

Certifique-se que o probe snmptd esteja configurado corretamente usando o seguinte método:

Na configuração do probe snmptd (clique duas vezes no probe snmptd no Infrastructure Manager), certifique-se de que a caixa de seleção **Remover aspas duplas** esteja marcada.



Link para o USM Exibe dispositivo incorreto

Válido em todas as plataformas

Sintoma:

Quando clico no ícone de lupa para "pesquisa do USM" na interface gráfica do usuário do Flow Analysis, estou vinculado ao dispositivo errado na visualização do USM.

Solução:

Se um dispositivo não for membro de um grupo no USM, o algoritmo de pesquisa do USM não poderá fazer uma correspondência exata e retornará a correspondência mais próxima que ele encontrar. Verifique no UMP se o dispositivo é membro de um grupo. Se não estiver no grupo, adicione-o a um grupo novo ou existente.

Coletor não mostrados no menu suspenso

Válido em todas as plataformas

Sintoma:

Quando clico no menu suspenso da barra superior para mostrar coletores disponíveis, nenhum é exibido, ou aquele desejado não é relacionado.

Solução:

Os Serviços de Descoberta não encontraram o probe do Coletor no sistema do Coletor. Pare e reinicie os probes Discovery_server e Discovery_agent do Infrastructure Manager.

Código de mensagem de erro 500

Sintoma:

Recebo o código de mensagem de erro 500.

Solução:

Os serviços de monitoramento não conseguem localizar probes. Isso pode significar que o discovery_server não está em execução. Mesmo que o próprio probe não está sendo executado e aparecerá (marcado em laranja/vermelho) na lista de detecção.

Código de mensagem de erro 400

Sintoma:

Recebo o código de mensagem de erro 400.

Solução:

Não é possível se comunicar com o probe. Isso ocorre quando o probe não está sendo executado ou não é possível se comunicar com ele.

Código de mensagem de erro 200

Sintoma:

Recebo o código de mensagem de erro 200.

Solução:

O probe responde com um conjunto de dados vazio. Isso pode acontecer se não houver dados disponíveis para o intervalo de tempo selecionado ou se a hora do sistema definida no sistema NetQoS estiver incorreta.