CA Nimsoft Monitor

Guia de Introdução

7.5

Histórico de revisões do documento

Versão	Data	Alterações
7.5	Março de 2014	Não há revisões.
7.1	Dezembro de 2013	Não há revisões.
7.0	Setembro de 2013	Revisado para o NMS 7.0.
6.5	Março de 2013	Revisões mínimas do NMS 6.5
6.2	Dezembro de 2012	Revisões e ajustes na documentação do NMS 6.20
6.1	Setembro de 2012	Revisões mínimas e correções da documentação do NMS 6.1.
3.0	Junho de 2012	Revisado para o NMS 6.0.
2.0	Outubro de 2011	Simplificado e revisado.
1.0	Junho de 2010	Versão inicial do *Guia de Introdução do Nimsoft Server.*

Entrar em contato com a CA

Entrar em contato com a CA Support

Para sua conveniência, a CA Technologies oferece um site onde é possível acessar as informações necessárias a seus produtos da CA Technologies para escritório doméstico, pequena empresa e corporativos. Em http://ca.com/support, é possível acessar os seguintes recursos:

- Informações para contato online e telefônico, assistência técnica e atendimento ao cliente
- Informações sobre fóruns e comunidades de usuário
- Downloads de produto e documentação
- Políticas e diretrizes de CA Support
- Outros recursos úteis adequados ao seu produto

Fornecendo comentários sobre a documentação do produto

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

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

Avisos legais

As informações legais sobre software de domínio público e de terceiros usado na solução do Nimsoft Monitor estão documentadas em *Licenças de Terceiros e Termos de Uso do Nimsoft Monitor (*http://docs.nimsoft.com/prodhelp/en_US/Library/Legal.html*).*

Índice

Capítulo 1: Introdução

Visão geral da solução

O CA Nimsoft Monitor é uma solução de gerenciamento de rede que permite monitorar e gerenciar o desempenho e a disponibilidade em ambientes complexos. A arquitetura flexível, modular e escalonável permite adicionar com rapidez novos recursos de monitoramento de TI, conforme a sua infraestrutura se desenvolve.

Recursos

O Nimsoft Monitor está disponível sob demanda ou no local. Qualquer um dos modelos de uso fornece recursos de monitoramento completos. Por exemplo, o Nimsoft Monitor pode:

- Monitorar todas as portas em todos os servidores, hubs, comutadores e roteadores no seu ambiente de TI
- Detectar redes TCP/IP, exibir topologias, monitorar a integridade da rede e coletar dados de desempenho, de modo que seja possível identificar rapidamente o motivo raiz das falhas de rede
- Fornecer notificações e painéis em tempo real sobre as interrupções
- Integrar-se com perfeição ao CA Nimsoft Service Desk.

Benefícios

A infraestrutura robusta do Nimsoft Monitor e suas ferramentas de gerenciamento fáceis de usar fornecem diversos benefícios para os usuários. Com essa solução, é possível:

- Configurar sua infraestrutura de monitoramento e exibir os dados a partir de qualquer lugar na rede
- Fazer uma busca detalhada nas métricas do dispositivo e nos relatórios de desempenho
- Gerenciar as áreas da rede que são segmentadas por firewalls altamente restritivos
- Compartamentalizar ou restringir as ações do operador e exibições da rede
- Manter o inventário do dispositivo para o gerenciamento de ativos
- Desenvolver relatórios sobre tendências da rede e analisar dados da rede

Componentes

O Nimsoft Monitor é composto pelos seguintes produtos:

- **Nimsoft Monitor Server**, que inclui o software distribuído que monitora seu ambiente de TI e controla os dados e o banco de dados que armazena os dados
- **Gerenciador de infraestrutura**, uma interface com base no Windows para a configuração e o gerenciamento do sistema Nimsoft
- **Console de administração**, um console de gerenciamento com base em navegador que fornece muitos dos mesmos recursos do Gerenciador de infraestrutura
- **Unified Management Portal** (UMP), um portal com base na web que permite detectar dispositivos e exibir dados, alarmes e mensagens de várias maneiras

Sobre este guia

Este guia fornece uma visão geral da solução CA Nimsoft Monitor. Ele é destinado a administradores de sistemas, profissionais de TI e gerentes de negócios que precisam ter um entendimento básico dos componentes do Nimsoft Monitor e de como eles funcionam em conjunto.

Este guia concentra-se em quatro áreas do Nimsoft Monitor:

- Nimsoft Monitor Server (na página 13), fornece uma introdução ao monitoramento do Nimsoft. Descreve os componentes da infraestrutura, o fluxo de mensagens e a segurança do sistema.
- Unified Management Portal (na página 25), apresenta o UMP, uma interface personalizável com base na web, onde é possível exibir alarmes e mensagens, monitorar e gerenciar sistemas de computador, criar e exibir relatórios e executar muitas outras tarefas.
- Gerenciador de infraestrutura (na página 31), oferece uma visão geral da interface do Nimsoft para a configuração e o gerenciamento do seu sistema Nimsoft.
- O Console de administração apresenta o console de gerenciamento com base em navegador, uma alternativa ao Gerenciador de infraestrutura
- Alarmes do Nimsoft, tópico que fornece uma introdução sobre como os alarmes são criados e tratados.

Para obter mais informações, consulte os seguintes documentos, disponíveis na biblioteca de documentação da Nimsoft ou na guia **Downloads**, em support.nimsoft.com:

- *Guia de Instalação do Nimsoft Monitor Server*
- *Guia de Configuração do Nimsoft Monitor Server*
- *Guia do Infrastructure Manager do Nimsoft Monitor Server*
- *Guia de Introdução ao Console de Administração do Nimsoft Monitor*
- *Informações do usuário do Unified Management Portal do Nimsoft Monitor*
- *Notas da Versão e Guia de Atualização do NMS*

Capítulo 2: Nimsoft Monitor Server

A coleta e o armazenamento de dados são processados pelo Nimsoft Monitor Server (NMS). Os componentes distribuídos do NMS funcionam em conjunto para monitorar falhas e desempenho. Esta seção descreve os componentes, explica como eles funcionam em conjunto e, em seguida, fornece cenários que mostram como eles podem ser distribuídos por várias implantações.

Esta seção contém os seguintes tópicos:

Sistemas com suporte

O software de monitoramento e servidor NMS é suportado nos sistemas Windows, Linux e Solaris. O software de monitoramento também é suportado nos sistemas AIX e HP-UX. Para obter uma lista completa de sistemas operacionais, bancos de dados e navegadores suportados, consulte a Matriz de suporte de compatibilidade da Nimsoft.

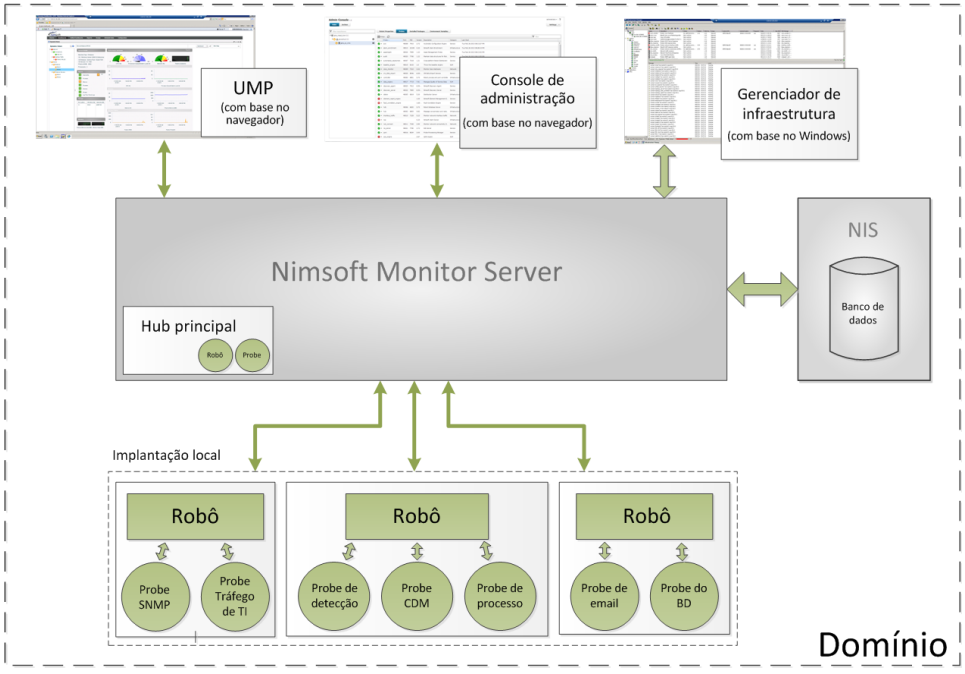
Arquitetura de sistema

A arquitetura do sistema Nimsoft Monitor consiste na infraestrutura, que é o software distribuído que monitora o seu ambiente de TI e controla os dados, e no NIS (Nimsoft Information Store - Repositório de informações do Nimsoft), o banco de dados que armazena os dados.

Todos os componentes da infraestrutura são organizados em uma hierarquia. De cima para baixo, os componentes são:

- Probes
- Robôs
- Hub
- Domínio

A ilustração a seguir mostra um domínio do Nimsoft, abrangendo o servidor, o banco de dados, os consoles de gerenciamento e a infraestrutura (hub, robôs e probes):



Os componentes permitem personalizar a sua configuração de monitoramento e organizar o fluxo de dados.

Probes

Um *probe* é um pequeno segmento de software que executa uma tarefa dedicada. Na parte inferior da hierarquia, eles podem ser considerados como conectores e operadores dentro do NMS. O Nimsoft tem dois tipos de probes:

- **Probes de monitoramento**, que coletam dados de desempenho e disponibilidade. Alguns probes coletam dados dos computadores nos quais residem. Os probes remotos monitoram dispositivos externos a si próprios, como comutadores e roteadores de rede.
- **Probes de serviço** (também chamados de probes de utilitário ou de infraestrutura), que fornecem funções de utilitário do produto para o NMS.

Os probes podem ser facilmente configurados para os seus próprios requisitos de monitoramento específicos. Por exemplo, é possível configurá-los para serem executados em um horário específico (probe programado) ou continuamente (probe contínuo). Cada probe mantém seu próprio arquivo de configuração.

As ferramentas do Nimsoft permitem a implantação fácil e eficiente de probes para os *robôs*, o próximo componente na hierarquia do Nimsoft.

Probes personalizados

As soluções prontas da Nimsoft fornecem um início rápido e, normalmente, atendem a cerca de 80% das necessidades de monitoramento de servidores e estações de trabalho na maioria das organizações.

Como os 20% restantes variam de site para site, o Nimsoft permite que você desenvolva suas próprias soluções, que são direcionadas diretamente para os problemas que causam a maioria das perturbações. O Nimsoft Software Development Kit (SDK) permite que você desenvolva probes e utilitários que se integrem com o seu ambiente do Nimsoft. O SDK está disponível para as seguintes linguagens de programação:

- Perl
- C
- Java
- Visual Basic/.NET

Robôs

Os *robôs* gerenciam os probes. Um robô inicia e interrompe seus probes nos horários exigidos, além de coletar, enfileirar e encaminhar os dados de monitoramento. Um robô é instalado em cada computador que se deseja monitorar.

Cada robô tem três tarefas dedicadas:

- **Controlar os probes** vinculados ao robô, o que inclui iniciá-los e interrompê-los nos horários requeridos (realizado com o probe *controlador* do robô).
- **Coletar, enfileirar e encaminhar** as mensagens do probe (realizado com o probe do *spooler*).
- **Fornecer um serviço de banco de dados simples** para seus probes. Isso permite que o robô armazene dados para o monitoramento de limite e das tendências dos dados, e garante que os dados coletados sobrevivam às interrupções de energia (realizado com o probe *hdb*).

Os três probes mencionados aqui são os probes de serviço que estão presentes em todos os robôs do Nimsoft.

Todos os robôs são basicamente idênticos; são as coleções de probes que eles gerenciam que os diferenciam. Os probes podem ser agrupados em pacotes, de modo que seja possível implantá-los apropriadamente em vários tipos de servidores.

Se um robô tiver um probe do hub, ele será promovido para o próximo nível na hierarquia do Nimsoft: o *Hub*.

Hubs

Um *hub* é um robô que tem responsabilidades adicionais. Da mesma forma como um robô gerencia seus probes, o hub gerencia os seus robôs. Toda implantação do Nimsoft tem um ou mais hubs. Todos os hubs executam estas tarefas:

- **Coletar todas as mensagens** provenientes dos robôs
- **Expedir rapidamente as mensagens** para assinantes conectados e/ou filas
- **Manter as informações do sistema**, como tabelas de nomes

Os hubs têm as designações a seguir, dependendo de suas finalidades:

- O **hub principal** se comunica com o banco de dados. Toda implantação tem um, e somente um, hub principal. Esse hub é criado ao instalar o software do servidor do NMS.
- **Hubs secundários** podem ser usados para verificar a rede (detecção de dispositivos), executar cálculos da linha de base em métricas de QoS ou agrupar robôs de acordo com a função, a localização geográfica, o código do departamento, entre outros critérios. Embora os hubs secundários sejam opcionais, quase todas as implantações os possuem. Os hubs secundários são criados após o software do servidor do NMS estar instalado. Eles podem ser criados ou removidos, conforme necessário, para atender às necessidades do seu ambiente de TI.
- Um **hub de failover** é um hub secundário que executa as ações do hub principal caso este mude de estado (torne-se indisponível).
- Os **hubs de encapsulamento** usam conexões do tipo VPN para comunicação pelos firewalls.
- Um **hub de relay** é instalado em uma implantação do Nimsoft ITMaaS. Ele se comunica com o serviço do Nimsoft.

Domínio

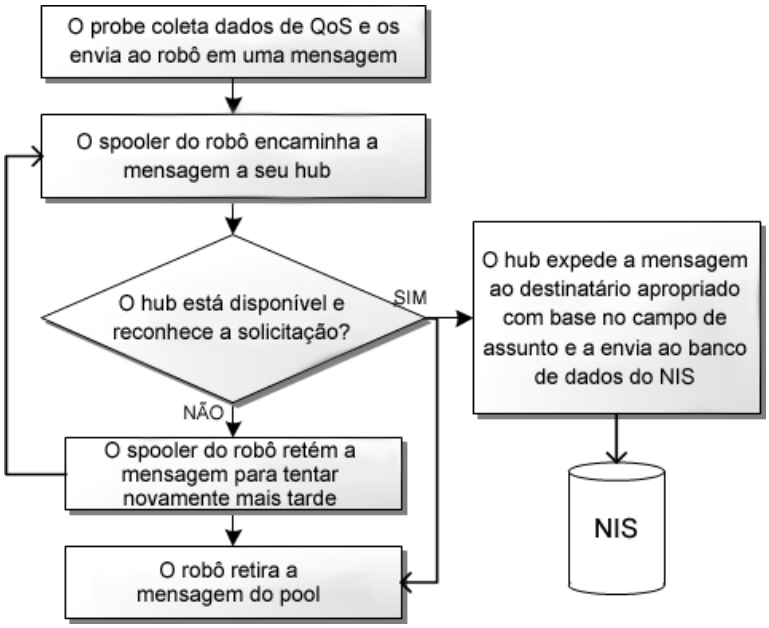
O *domínio* é um conjunto lógico no qual todos os componentes da infraestrutura do Nimsoft são agrupados.

O domínio é criado ao instalar o software do servidor do NMS. Um site geralmente é configurado com um domínio. Vários aspectos de segurança, como perfis de usuário, permissões e direitos de acesso, são distribuídos no domínio.

Fluxo de mensagens

Visão geral

O diagrama a seguir mostra como os dados são transferidos de um probe para o banco de dados.



As seções a seguir explicam os elementos envolvidos na transferência de dados.

Barramento

O barramento de mensagens do Nimsoft fornece um conjunto de serviços para os robôs, hubs, banco de dados e os consoles de gerenciamento. O fluxo de mensagens no barramento é gerenciado usando roteamento e esquemas de nomenclatura.

Modelo de mensagem

O fluxo de mensagens se baseia em modelos de solicitação/resposta e de publicação/assinatura:

- **Solicitação/resposta** é o modo padrão de comunicação na rede. Um cliente emite uma solicitação para um servidor e o servidor responde à solicitação.
- **Publicação/assinatura** permite que clientes enviem dados," como alertas, dados de desempenho ou mensagens direcionadas para servidores de gateway, sem um destinatário designado. Também permite que os clientes selecionem as mensagens com base no assunto.

Mecanismo de assinatura

O mecanismo de assinatura permite que probes e robôs selecionem as mensagens com base no assunto, e não no endereço do remetente. Um cliente que está configurado para receber mensagens do Nimsoft envia uma solicitação de assinatura para o hub. O cliente recebe então mensagens que correspondem aos assuntos assinados do hub. Um cliente pode usar os seguintes métodos para se inscrever:

- **Assinar** - o cliente se conecta ao hub e recebe mensagens desde que o cliente esteja em execução.
- **Anexar** - o hub configura uma fila de mensagens para armazenar as mensagens se o cliente não estiver em execução. Quando o cliente for reativado, todas as mensagens serão repassadas, incluindo aquelas que foram recebidas quando o cliente estava inativo.

Filas de mensagens

As *Filas de mensagens* transferem mensagens de e para os hubs. As filas se enquadram em duas categorias:

- Filas **permanentes**, são armazenadas no banco de dados do hub local e sobrevivem ao reinício do hub. Esse tipo de fila garante que as mensagens sejam entregues, mesmo que o destinatário esteja desativado quando uma mensagem for gerada.

  Exemplo: probe do NAS (Nimsoft Alarm Server - Servidor de alarmes do Nimsoft). Se o hub que executa esse serviço ficar inoperante e, em seguida, voltar a funcionar, ele busca todos os alarmes gerados enquanto ele estava inoperante. Isso garante que nenhum alarme seja perdido.

- Filas **temporárias**, são usadas para caminhos de comunicação menos críticos.

  Exemplo: o portlet visualizador de alarmes do UMP. Quando um usuário inicia o UMP, o portlet faz assinaturas em mensagens de alarme e uma fila temporária é criada. As mensagens são encaminhadas para essa fila enquanto o visualizador de alarmes está ativo. Quando o visualizador está fechado, a fila é removida.

As filas são configuradas em dois modos:

- **Automaticamente**: na maioria das situações envolvendo um único domínio/sub-rede, as filas são uma parte transparente e automática da infraestrutura. As filas permanentes são configuradas entre os hubs durante a instalação. As filas temporários são criadas conforme necessário.
- **Manualmente**: usando o Gerenciador de infraestrutura, é possível criar filas adicionais entre os hubs, de acordo com a necessidade. É possível implantar as seguintes filas ao adicionar hubs secundários:
  - Alarme – com vários hubs secundários, é possível configurar uma fila para enviar todos os alarmes para um determinado hub secundário.
  - QoS – com vários hubs secundários, é possível encaminhar mensagens de QoS para o hub principal. Observe que a instalação do NAS em um hub irá criar a fila necessária automaticamente.
  - Detecção – com vários hubs secundários hospedando agentes de detecção, os dados coletados da detecção de dispositivos devem chegar ao hub principal em que o servidor de detecção está hospedado. Você deve configurar filas do probe_discovery em todos os hubs que existem ao longo deste caminho de comunicação. Para obter detalhes, consulte a seção "Configurar filas do probe_discovery" no *Guia do Usuário de Detecção*, disponível na Biblioteca de documentação do Nimsoft.
  - Linhas de base – com um ou mais probes baseline_engine hospedados em hubs secundários, você deve configurar as filas do qos_baseline para rotear os dados da linha de base para o hub principal. Consulte a seção Implantação recomendada do probe em vários hubs (vários níveis) na ajuda online do probe baseline_engine, disponível na biblioteca de documentação do Nimsoft.

O serviço de nome

Cada controlador do robô mantém uma lista de:

- Todos os probes controlados pelo robô.
- Todos os probes *ativos* (probes que detectam uma porta vinculada e respondem a um conjunto de comandos). Essa lista é distribuída para o hub mediante solicitação. Por exemplo, o Infrastructure Manager solicita com frequência essas informações.

Os nomes encontrados nessas tabelas são a base para a resolução de porta nome para IP e constituem o que definimos como um endereço do Nimsoft. Um cliente pode consultar o controlador para buscar uma resolução de nome/IP de maneira semelhante à consulta no DNS ou WINS, com base no nome do serviço (por exemplo, NAS).

Segurança do sistema

A segurança do sistema é garantida por meio de:

- **Acesso** -" Quem tem permissão para fazer o quê?
- **Autenticação** - O cliente é quem ele afirma ser?
- **Criptografia** - É possível impedir que outras pessoas leiam os dados?

Listas de controle de acesso (ACLs)

É necessário efetuar logon para acessar a infraestrutura e os dados de monitoramento do Nimsoft. As ACL (Access Control Lists - Listas de controle de acesso) permitem restringir ainda mais as permissões de usuário. O administrador do Nimsoft pode:

- **Anexar contas de usuário** a uma das cinco ACL padrão: Superusuário, Administrador, Operador, Criador de painéis e Convidado. As permissões predefinidas para essas ACL (exceto para Superusuário) podem ser ainda mais restritas.
  - Novos usuários são criados no **Gerenciador de infraestrutura** ou no **UMP**.
  - As ACLs são administradas em **Gerenciador de infraestrutura** > **Segurança** > **caixa de diálogo Gerenciar ACL**.
- **Criar novas ACLs** com permissões personalizadas.
- **Configurar o hub** para encaminhar as solicitações de logon para um servidor LDAP e para acessar o recipiente com os grupos de usuários.

SID (Session Identification - Identificação de sessão)

As *identificações de sessão* (ou SIDs) permitem que usuários e probes executem comandos. Qualquer solicitação deve ter uma SID válida.

Cada usuário recebe uma SID após o logon.

Segurança do console

O acesso ao console com base na web pode ser protegido com autenticação usando certificados SSL e transferência de dados criptografados por HTTPS.

Console de administração

Por padrão, o Console de administração se conecta ao servidor do Nimsoft Monitor por HTTP. Ele pode ser configurado para se conectar com segurança a HTTPS, usando um certificado autoassinado ou um certificado SSL assinado por autoridades. Para obter detalhes, consulte a seção Gerenciar segurança na ajuda online do Console de administração, disponível na biblioteca de documentação do Nimsoft.

UMP (Unified Management Portal)

Para obter informações sobre como configurar o UMP para se comunicar com segurança, consulte o *Guia de Implementação HTTPS* do UMP, disponível na biblioteca de documentação do Nimsoft.

Segurança do probe

Os probes podem ser categorizados como simples ou complexos:

- A maioria dos probes tem tarefas simples, como monitorar o desempenho e enviar um alarme se um limite for atingido. Esses probes não precisam de um SID, pois eles só enviam mensagens.
- Outros têm tarefas mais complexas, como coletar informações de, e executar comandos em, outros probes. Esses probes precisam de permissão para conectar e executar comandos em probes remotos. Por isso, são um possível risco para a segurança.

Para que um probe obtenha uma SID, duas condições devem ser atendidas:

1. O probe deve ser instalado em um robô para gerar uma soma de verificação assinada. Isso requer direitos de administração e não pode ser executado por intrusos ou operadores.
2. O controlador deve iniciar o probe. Um esquema de número mágico garante que isto não possa ser contornado.

Se esses requisitos forem atendidos, o controlador do robô se conecta ao hub para obter a SID adequada para o probe. Isso exige que o probe tenha sido adicionado à configuração de segurança com as permissões apropriadas e uma máscara IP.

Monitoramento pelos firewalls

Atualmente, a maioria das empresas tem um ou mais firewalls em sua rede, internamente entre diferentes redes e externamente para a internet ou uma DMZ de rede.

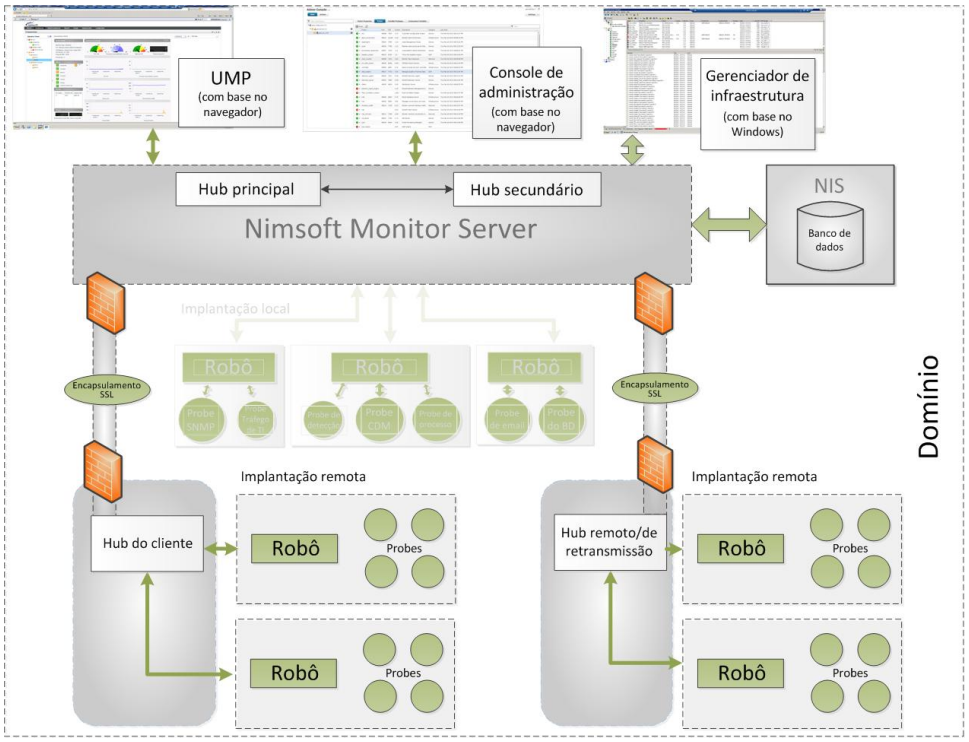
Como os administradores de rede normalmente relutam em abrir um firewall para uma série de endereços IP e portas que os aplicativos de gerenciamento exigem, pode ser difícil administrar e monitorar toda a rede a partir de um local central.

A solução é configurar um encapsulamento Secure Shell (SSH) entre dois hubs separados por um firewall. O encapsulamento configura uma conexão VPN (Virtual Private Network - Rede virtual privada) entre os dois hubs. Todas as solicitações e mensagens são roteadas por meio do encapsulamento e expedidas no outro lado. Esse roteamento é transparente para os usuários.

Você pode criar encapsulamentos entre qualquer hub do Nimsoft.

O assistente da DMZ o ajudará a configurar encapsulamentos com facilidade entre os hubs. Para obter mais instruções:

- Consulte no *Guia de Instalação do Nimsoft Monitor Server* a seção sobre "Instalação de DMZ"*,* disponível pela biblioteca de documentação da Nimsoft ou pela guia **Downloads**, em support.nimsoft.com.
- No Gerenciador de infraestrutura, clique duas vezes no probe do hub para abrir sua GUI e, em seguida, acesse a ajuda online pressionando o botão **Ajuda**. A seção "A guia Encapsulamentos" (também disponível online) aborda o servidor de encapsulamento e a configuração do cliente.


UMP
(com base no navegador)
Console de administração
(com base no navegador)
Gerenciador de infraestrutura
(com base no Windows)
Hub principal
Hub secundário
Nimsoft Monitor Server
NIS
Banco de dados
Implantação local
Robô
Encapsulamento SSL
Encapsulamento SSL
Domínio
Implantação remota
Implantação remota
Hub do cliente
Robô
Probes
Robô
Probes
Hub remoto/de retransmissão
Robô
Probes
Robô
Probes

Capítulo 3: Unified Management Portal

O UMP (Nimsoft Unified Management Portal) é uma interface com base na web que permite:

- Verificar a rede (detecção) ou importar dados do dispositivo a partir de uma origem externa, como um CMDB
- Monitorar e gerenciar sistemas de computador
- Criar gráficos de dados de QoS
- Exibir e gerenciar alarmes
- Criar SLAs e exibir seus relatórios de desempenho
- Criar, exibir e agendar relatórios
- Criar e visualizar painéis personalizados
- Abrir e gerenciar tickets do Service Desk
- Gerenciar usuários

Observação: a documentação do UMP está disponível na ajuda online do produto.

Esta seção contém os seguintes tópicos:

Portlets UMP

A seguir estão listados muitos dos aplicativos ou portlets disponíveis no UMP. Para obter mais informações sobre cada um deles, consulte a documentação do usuário do UMP.

- **Administração da conta**, permite criar, modificar ou excluir usuários. Pode-se também definir as senhas para usuários.
- **Console de alarmes**, permite exibição completa, filtragem e gerenciamento de alarmes.
- **Monitor de experiência do usuário com a nuvem**, permite monitorar sites e serviços em nuvem de todo o mundo, e mede o status de suas transações e serviços de mais de 60 locais.

- **Painéis personalizados**, permitem:
  - Acessar os painéis personalizados que exibem os dados de QoS e alarmes de sistemas monitorados em sua rede
  - Exibir os alarmes
  - Visualizar as Exibições dinâmicas, que exibem o estado (nível de alarme, desempenho, etc.) dos sistemas monitorados em sua rede
- **Criador de painéis**, permite criar painéis personalizados.
- **Status da detecção**, exibe um gráfico de pizza mostrando o status da detecção de sistemas em sua rede. A detecção pesquisa constantemente a sua rede em busca de sistemas de computador e atualiza o diagrama para mostrar o status atual. Clique no gráfico para exibir informações adicionais do sistema.
- **Exibições dinâmicas**, exibem painéis de QoS gerados automaticamente para os sistemas detectados em sua rede. No painel da árvore de portlet, é possível selecionar um sistema para ver informações adicionais.
- **Visualizador de listas**, exibe dados (texto, números, medidores, alarmes ou gráficos) em um formato de tabela.
- **Criador de listas**, permite criar listas para serem exibidas no portlet Visualizador de listas.
- **Modo de manutenção**, permite interromper temporariamente o monitoramento de sistemas selecionados. As configurações de monitoramento são mantidas para que o monitoramento seja retomado quando o modo de manutenção encerrar.
- A **Administração remota do Nimsoft** é um console de gerenciamento para detecção e dados de configuração. Ele permite especificar as propriedades de monitoramento para os sistemas detectados na rede.
- **Gráfico de QoS**, fornece uma representação visual de dados de QoS. Selecione o host, a medição de QoS, o destino, o intervalo de tempo e os dados a serem exibidos em um gráfico. Também é possível exibir várias medições em um único gráfico, exibir vários gráficos de uma só vez e salvar um conjunto de gráficos como um relatório.
- **Visualizador de relacionamento,** exibe os relacionamentos entre os dispositivos na rede em diagramas visuais e intuitivos. Ele também executa a RCA (Root Cause Analysis - Análise do motivo raiz) para determinar o dispositivo que está causando uma interrupção e suprime os alarmes dos nós dependentes.

- **Relatórios**, exibem:
  - Relatórios de qualidade de serviço (QoS), que devem ser criados manualmente usando a GUI do probe report_engine. Esta GUI é iniciada clicando duas vezes no probe report_engine no Infrastructure Manager. Consulte a documentação online do probe do Nimsoft para obter detalhes sobre o report_engine.
  - Relatórios de SLA (Service Level Agreement - Acordo de Nível de Serviço), que são gerados automaticamente para os SLA criados no Gerenciador de nível de serviço.
- **Relatórios unificados**, fornecem um conjunto abrangente de ferramentas do Business Intelligence (BI) que fornecem geração de relatórios estáticos e interativos, e recursos de análise de dados. Os relatórios unificados oferecem suporte ao painel arrastar e soltar, gráfico integrado, relatório web, programação do relatório, distribuição e versão histórica.
- O **USM (Unified Service Monitoring - Monitoramento de Serviços Unificados)** fornece o Assistente de detecção para a automação da entrada de dispositivos, bem como visualizações de sistemas monitorados para os usuários finais, organizadas de acordo com a conta do usuário.
- **Conteúdo da web**, permite se vincular a uma página da web.

Criador de painéis

O aplicativo Criador de painéis é a área para criar e acessar os painéis. É possível criar painéis para monitorar sistemas de computador na rede para dados e alarmes de QoS usando vários widgets modelo, como objetos do alarme, objetos do marcador, gráficos e tabelas:

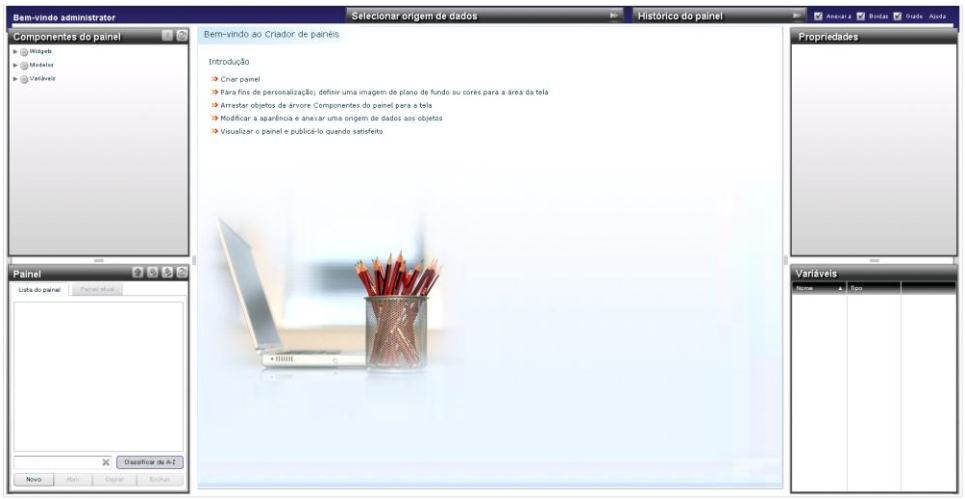
- Os objetos do alarme podem ser filtrados para refletir o estado dos computadores que desejar.
- Os objetos do marcador podem ser conectados em diferentes origens de dados (QoS, probes, variáveis, etc.).
- Os painéis podem ser usados para criar painéis com vários níveis em uma estrutura de árvore.
- Os objetos da tabela podem ser usados se desejar apresentar a saída de uma consulta ao NIS, em forma de tabela, em um painel.

O layout dos componentes do painel e o canvas de plano de fundo podem ser configurados com uma ampla variedade de cores, fontes, sons e origens de dados.

Pode-se também importar e usar em um dos modelos de painel disponível. Há quatro modelos de painéis disponíveis; dois para os dispositivos de rede e dois para os sistemas do servidor.

Pode-se também encontrar vários objetos gerais, como objetos de texto, de imagens, etc. O Criador de painéis também contém uma ferramenta de visualização que permite visualizar a aparência e o layout do painel antes de publicá-lo.

Os painéis estarão disponíveis no Unified Monitoring Portal quando forem salvos e publicados. Nesse local, é possível visualizar o estado e os valores de QoS dos sistemas monitorados bem como gerenciar os alarmes.



A janela Criador de paineis contém as seguintes seções principais:

Painéis

Esta seção, localizada no canto inferior esquerdo, permite abrir, editar ou copiar os paineis existentes, bem como criar um painel. É possível até mesmo fazer download de um ou mais modelos de paineis, modificá-los e usá-los como seu próprio painel. A seção também contém a funcionalidade para publicar os painéis, disponibilizando-os na lista de painéis.

Componentes do painel

Esta seção contém os blocos de construção ou widgets (objetos) que podem ser usados ao criar os painéis. Basta arrastar e soltar os objetos ou modelos no painel que está sendo editado ou criado. Os objetos podem ser componentes do alarme, marcadores, paineis, etc.

Além dos widgets, há um nó chamado Modelos. É possível salvar um objeto como um modelo. Se tiver configurado um objeto e deseja salvar e usá-lo no futuro ao criar outros paineis, clique com o botão direito do mouse no objeto e selecione a opção Salvar como modelo

Histórico do painel

Esta seção contém a funcionalidade para registrar as alterações feitas no painel atual no canvas. Oferece suporte ao mecanismo de desfazer/refazer de algumas operações; em geral, para adicionar, excluir, redimensionar e mover objetos.

Propriedades

Esta seção contém as propriedades disponíveis para o objeto selecionado. Ao criar um painel, arraste objetos da seção Componentes do painel e solte-os no canvas. Ao selecionar um objeto no canvas, as propriedades disponíveis para o objeto selecionado serão exibidas na seção Propriedades. Configure os objetos atribuindo as propriedades que desejar.

Painéis personalizados

É possível criar painéis personalizados usando o Criador de painéis. Os painéis que você vê depende das permissões definidas na ACL para sua conta de usuário.

Painel

Na estrutura de árvore, a cor dos ícones representa a gravidade mais alta para os objetos do alarme nos painéis. Clique duas vezes em um ícone e o painel correspondente será iniciado no painel.

Os painéis podem conter marcadores, objetos de alarme, medidores, gráficos, tabelas, painéis, entre outros.

Os objetos painel e alarme refletem o nível de gravidade do alarme com a gravidade mais alta. Clicar duas vezes em um objeto exibe a lista de alarmes, permitindo gerenciá-los.

Ferramenta Mini Map

Esta ferramenta amplia uma área de um painel. Uma versão minimizada do painel é mostrada na janela Mini Map. Um controle deslizante permite aumentar ou diminuir o painel na tela.

Gerenciando alarmes em painéis

Se o painel contém objetos do alarme, é possível exibir a lista de alarmes relacionados ao clicar duas vezes em um ícone do alarme que não seja verde (não há alarmes associados a objetos verde).

Capítulo 4: Gerenciador de infraestrutura

A interface do Infrastructure Manager

A janela do Infrastructure Manager tem os seguintes elementos.

- **Menu principal** e **barra de ferramentas**. Os menus suspensos e os botões de acesso rápido permitem personalizar a exibição da interface, localizar elementos de infraestrutura e gerenciar contas de usuário.
- **Painel do console** (à esquerda). Esse painel fornece uma exibição hierárquica de sua infraestrutura e usa ícones codificados por cor para indicar o status dos elementos. Esse painel contém os seguintes nós:
  - **Domínios**, mostram a estrutura hub-robô-probe
  - **Exibições dinâmicas**, agrupam os robôs por sistema operacional
  - **Grupos**, exibem grupos de hubs, robôs ou probes criados pelo usuário
  - **Arquivo de dados**, permite acessar pacotes de probe e licenças armazenados no arquivo de dados do hub atual
  - **URLs** e **Aplicativos** permitem iniciar páginas da web ou outros aplicativos.
- **Painel da janela principal** (canto superior direito). Este painel exibe detalhes sobre o elemento selecionado no painel do console. Por exemplo, se você clicar em um hub no painel do console, todos os robôs do hub serão exibidos no painel da janela principal.

  Este painel também possui a sua própria barra de ferramentas dinâmica, a qual fornece acesso rápido às funções relacionadas aos elementos exibidos.
- **Painel de documento** (canto inferior direito). Esse painel é exibido se a opção de menu **Exibir > Painel do Dock** estiver marcada. É possível exibir:
  - Alarmes do Nimsoft
  - Mensagens do sistema
  - O conteúdo do painel da janela principal
  - Janelas ancoradas anteriormente.

Capítulo 5: Console de administração

Como alternativa ao Gerenciador de infraestrutura, o Console de administração fornece um número crescente de recursos de gerenciamento equivalentes. A interface gráfica do usuário com base no navegador permite gerenciar a infraestrutura do Nimsoft em praticamente qualquer sistema operacional do servidor ou desktop. Também é possível executar o console de administração em um portlet no UMP.

Os administradores de sistema do NMS e os usuários do NMS com permissões de administrador ou de superusuário podem acessar o Console de administração.

O Console de administração (acessível em um navegador da web ou em modo autônomo) é instalado e fica disponível após a instalação do sistema do NMS ser concluída. Para acessá-lo, use o link fornecido na página web do NMS (http://<*nome_ou_endereço_IP_do_servidor*>:8080): **Gerenciamento (Console de administração)**. O portlet Console de administração é instalado durante a instalação do UMP.

Por padrão, o Console de administração se conecta ao servidor por HTTP. Ele pode ser configurado para se conectar com segurança a HTTPS, usando um certificado autoassinado ou um certificado SSL assinado por autoridades. Os recursos de segurança, além de outros tópicos, são descritos em mais detalhes na ajuda online, disponível na biblioteca de documentação do Nimsoft.

Esta seção contém os seguintes tópicos:

Interface do Console de administração (na página 33)

Interface do Console de administração

O Console de administração tem os seguintes elementos.

- **Janela principal**: fornece uma visualização da infraestrutura. A janela principal está dividida em duas seções.
  - O painel de navegação esquerdo exibe os hubs e os robôs em uma estrutura de árvore.
  - O painel direito exibe informações de probes ou robôs com base em sua seleção no painel de navegação.
  - Na parte superior de cada seção existe um filtro que é usado para personalizar a exibição da interface.

- O botão **Infraestrutura** no canto superior esquerdo da janela principal. Clique nesse botão para exibir e configurar os componentes da infraestrutura.
  - Selecione um hub no painel de navegação para exibir, no lado direito da tela, as informações e propriedades do robô para aquele hub.
  - Selecione um robô no painel de navegação para visualizar, no painel direito, quatro opções para acessar informações sobre o robô: Propriedades do robô, Probes, Pacotes instalados e Variáveis de ambiente.
- O botão **Arquivo** no canto superior esquerdo da janela principal. Clique nesse botão para exibir e usar o arquivo do pacote de probes do Nimsoft.
  - Implante, importe, agrupe e exclua pacotes de probes nessa tela.
  - A tela *arquivo local* exibe os probes que residem no arquivo no hub. O arquivo local contém todos os probes instalados durante a instalação do NMS e aqueles que foram baixados posteriormente.
  - A tela *arquivo da web* exibe a lista de pacotes de probes no arquivo de suporte da Nimsoft.
  - A tela *atividade de distribuição* exibe um log de distribuições de pacotes de probes, juntamente com o status de cada distribuição.

Capítulo 6: Alarmes do Nimsoft

Os probes de monitoramento de alarmes verificam os computadores host em busca de sintomas de situações de erro. Isto pode ser por meio da verificação do espaço livre em disco, do conteúdo do arquivo de log, de problemas de desempenho ou de processos do sistema interrompidos. Quando um problema é encontrado, o robô envia uma mensagem que descreve o problema para o hub.

O Nimsoft fornece vários probes padrão que são projetados para monitorar uma ampla variedade de sistemas operacionais e aplicativos. A Nimsoft trabalha em estreita colaboração com os fornecedores desses sistemas para fornecer um monitoramento com foco nos problemas cotidianos que afetam os usuários e a equipe de suporte.

OBSERVAÇÃO: esta seção descreve os recursos disponíveis para um usuário com privilégios máximos. Algumas opções e botões do menu podem estar indisponíveis (esmaecidos) dependendo dos privilégios do usuário. Os alarmes que um usuário pode visualizar e as ações que podem ser executadas estão definidas na ACL.

Esta seção contém os seguintes tópicos:

Janela de alarmes

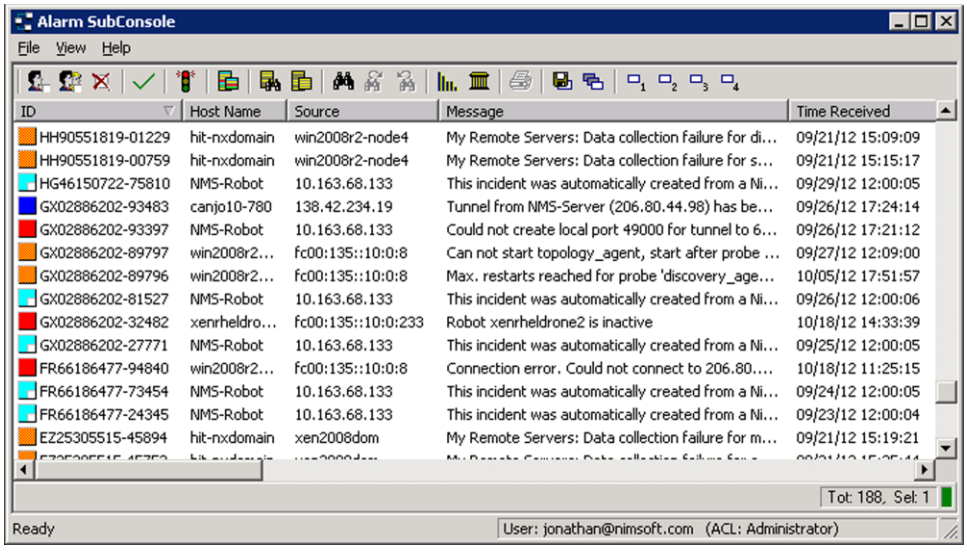
O console de alarmes, que é um componente do Infrastructure Manager e do UMP, permite que o usuário exiba e opere nos alarmes. O console é totalmente acionado por eventos e será atualizado automaticamente. Nesse console, é possível:

- Definir filtros complexos para obter rapidamente os subconjuntos de alarmes específicos
- Executar uma série de operações de gerenciamento com base em seus privilégios de usuário (criar e anexar observações, gerenciar ações e filtros ou definir alarmes nos estados visível /invisível)
- Aceitar e confirmar alarmes
- Exibir histórico de transações e consultar a funcionalidade com base em dados do histórico

O console exibe informações sobre os alarmes em formato de tabela. Os ícones da barra de ferramentas e as opções do menu permitem exibir informações e executar ações referentes aos alarmes.

Essa janela pode ser acessada de várias formas:

- No UMP como o portlet *Console de alarmes*
- No painel inferior direito do Infrastructure Manager
- Como o *Subconsole de alarmes*, um aplicativo autônomo iniciado a partir do Infrastructure Manager (mostrado aqui)



Para obter mais informações, consulte o *Guia do Usuário do Console de Alarmes*, disponível na guia **Downloads** em support.nimsoft.com.

Probe do Servidor de alarmes (NAS)

O NAS (Alarm Server - Servidor de alarmes) é um probe de serviço que recebe mensagens de alarme distribuídas pelo hub. Ele funciona da seguinte maneira:

1. Uma mensagem de alarme é gerada por um probe em algum lugar na infraestrutura da Nimsoft. Essa mensagem do tipo "transmissão" não tem destinatário especificado e pode ser recuperada por qualquer processo que tenha assinado o assunto do alarme.
2. O NAS, que assina o assunto do alarme, age na mensagem de entrada armazenando informações sobre o alarme em um banco de dados no subdiretório do NAS.
3. Quando os dados são solicitados (como quando um usuário exibe os alarmes no UMP ou no Infrastructure Manager), o servidor de alarmes envia os dados armazenados.

Este probe também:

- Oferece suporte à supressão de mensagens
- Oferece suporte ao aprimoramento de alarmes, com o qual as mensagens de alarme podem ser alteradas com base em regras definidas
- Fornece aos clientes eventos atualizados e serviços de repositório (obter, listar, fechar, etc.)
- Oferece suporte à filtragem de mensagens
- Oferece suporte a ações automáticas (operador automático)
- Fornece recursos de espelhamento
- Manipula mensagens de alarme

Manipulando alarmes

Os alarmes podem ser manipulados de várias maneiras. É possível:

- Trabalhar com eles no console de alarmes
- Instalar um gateway para encaminhar os alarmes para outras infraestruturas de sistemas de mensagens (email, GSM/SMS, pager ou mensagens SNMP)
- Integrá-los mais estreitamente a uma estrutura de gerenciamento de sistemas usando um dos kits de integração de estruturas disponíveis
- Manipulá-los automaticamente configurando perfis no *Operador automático* do probe do NAS

Todos os métodos garantem que os operadores sejam informados automaticamente sobre os problemas alguns segundos ou minutos após o sintoma aparecer.

Supressão de mensagens

Várias situações de erro no sistema monitorado podem resultar em um grande número de alarmes. Por exemplo, se o probe logmon monitorar um arquivo de log de um aplicativo que executa um loop infinito e registra erros no loop, um grande número de alarmes idênticos poderá ser gerado. Isto cria uma carga desnecessária no sistema, na rede e no servidor do NMS.

O mecanismo de supressão de mensagens permite evitar esse problema. Os modelos de supressão suportados pelo NAS são:

- Supressão **padrão**, um modelo simples que suprime mensagens com uma correspondência exata da ID do subsistema de mensagens, do nível de gravidade e do texto da mensagem.
- Supressão com **chave**, um modelo com base em uma chave de supressão que segue uma mensagem. Quando a supressão com chave é ativada, as mensagens com chaves de supressão correspondentes são suprimidas.

Confirmação automática

É possível usar a supressão com chave para limpar automaticamente a lista de alarmes quando o probe detectar que a situação crítica foi resolvida. Isso é feito por meio da ativação da confirmação automática com base em chaves. Isso significa que os alarmes com o nível de gravidade "limpo" automaticamente confirmam todos os alarmes anteriores com a mesma chave de supressão.

Por exemplo, uma configuração sensata do probe de monitoramento do disco seria enviar o primeiro alarme (95% cheio) com o nível de gravidade "grave", enquanto o último (55% cheio) poderia ter o nível de gravidade "limpo". Se o último alarme chegar, tudo estará de volta ao normal e o administrador não precisará responder ao primeiro alarme depois de tudo. O alarme será confirmado automaticamente pelo NAS, deixando o administrador com uma lista de tarefas pendentes com o menor número de "ruído" possível.

SID (Subsystem ID - ID do subsistema)

No Console de alarmes, os alertas são classificados por sua ID de subsistema, identificando com quais partes do sistema o alerta está relacionado. Esta é uma lista hierárquica de códigos, permitindo agrupar os alarmes de forma mais ampla ou mais restrita, conforme desejado.

Esta lista é armazenada no NAS. Se desenvolver ou personalizar probes, você pode definir sua própria lista de subsistemas. Esta lista também mapeia o código do subsistema em uma sequência de caracteres de texto para melhorar a legibilidade.

Arquivos de log de transações do alarme

É útil acompanhar a vida completa da mensagem a partir da mensagem inicial, através de várias supressões, até o fechamento da mensagem (confirmação). Um mecanismo de filtragem (ajustável pelo administrador) permite que o NAS registre todas as transações em um arquivo de log de transações específico.

Para manter o arquivo de log de transações o mais gerenciável possível, ele é automaticamente copiado em intervalos configurados. Os logs salvos são nomeados trans_*carimbo_de_data/hora*.log, onde *carimbo de data/hora* é a hora em que o arquivo foi criado (em segundos).

Use a ferramenta de configuração do NAS para exibir o log de transações ou ajustar as configurações.

Mensagens de notificação

Os seguintes tipos de mensagens são gerados:

- **alarm_new**: uma mensagem de alarme é recebida e a pegada da mensagem não foi registrada anteriormente
- **alarm_update**: uma mensagem de alarme é recebida e a pegada da mensagem já existe
- **alarm_close**: o cliente fechou (confirmação) um alarme e este foi removido dos alarmes ativos no momento

Todas as transações são registradas no arquivo de log de transações.

Apêndice A: Referência de permissões da ACL

O NMS inclui cinco modelos de ACL (Access Control List – Lista de Controle de Acesso) predefinidos, com as seguintes permissões:

Permissões	Administrador (super)	Criador de painéis (admin)	Convidado (aberto)	Operador (gravação)	Superusuário (super)	Descrição
Aceitar	S	S	-	S	S	Atribuir alarmes a si mesmo
Cancelar atribuição	S	S	-	-	S	Cancelar atribuição de alarmes
Estados de exibições dinâmicas	S	-	-	S	S	Acesso geral às informações sobre o estado do alarme Exibições dinâmicas
Alarmes invisíveis	-	S	-	-	S	Mostrar alarmes definidos como invisíveis
Reatribuir	S	S	-	-	S	Substituir atribuição em Atribuir/Confirmar
Histórico do alarme	S	S	-	S	S	Histórico de transações e consultas de alarmes
Confirmar	S	S	-	S	S	Fechar alarmes
Gerenciamento de alarmes	S	S	-	-	S	Vários recursos de gerenciamento de alarmes
Atribuir	S	S	-	-	S	Atribuir alarmes a outro usuário
Detalhes do alarme	S	S	S	S	S	Acesso geral a listas e detalhes de alarmes
Automação – Exibir itens	S	S	S	S	S	Não implementada
Automação – Alterar itens de configuração	S	S	-	S	S	Não implementada

Automação – Gerenciar fluxos de trabalho	-	-	-	-	S	Não implementada
Automação – Criar e modificar fluxos de trabalho	-	-	-	-	S	Não implementada
Criação de painéis	-	S	-	-	S	Criar, modificar e excluir painéis

Permissões	**Administrador**	**Criador de painéis**	**Hóspede**	**Operador**	**Superusuário**	**Descrição**
Detecção	-	S	-	-	S	Detectar e criar painéis modelos
Exibições dinâmicas	S	S	-	S	S	Visualizar exibições dinâmicas
Publicar na web	-	S	-	-	S	Gerenciamento do servidor HTML do Nimsoft
Upload de painéis	-	S	-	-	S	Fazer upload de painéis para o arquivo
Download de painéis		S	-	-	S	Fazer download de painéis do arquivo
Gerenciamento do arquivo	S	-	-	-	S	Criar e modificar pacotes
Segurança estendida	S	-	-	-	S	Vários recursos de manutenção de segurança
Modo de manutenção	S	-	-	-	S	Gerenciamento do modo de manutenção de robôs
Gerenciar ACL	S	-	-	-	S	Criar, modificar e excluir ACLs
Gerenciamento de licenças	S	-	-	-	S	Adicionar e excluir licenças do Nimsoft
Administração de usuário	S	-	-	-	S	Criar, modificar e excluir usuários

Administração do portal	S	-	-	-	S	Acesso à administração do portal da web
Modificar perfis	S	-	-	-	S	Modificar e salvar perfis de usuário
Distribuição	S	-	-	-	S	Distribuir pacotes de arquivamento
Opções do programa	S	S	-	-	S	Alterar vários atributos do programa
Gerenciamento básico	S	-	-	-	S	Reiniciar, mover, fazer download, ignorar, etc.

Permissões	**Administrador**	**Criador de painéis**	**Hóspede**	**Operador**	**Superusuário**	**Descrição**
Gerenciar perfis	S	-	-	-	S	Criar, renomear e excluir perfis de usuário
Ferramentas de gerenciamento	S	-	-	-	S	Várias ferramentas (localizar/conectar, etc.)
Gerenciamento do arquivo	S	-	-	-	S	Criar e modificar pacotes
Configuração do probe	S	-	-	-	S	Gerenciamento da ferramenta de configuração do probe
Nível de execução 1	S	-	-	-	S	Nível de execução 1 do comando do probe
Nível de execução 2	S	-	-	-	S	Nível de execução 2 do comando do probe
Nível de execução 3	S	-	-	-	S	Nível de execução 3 do comando do probe
Resumo de alarmes	S	S	S	S	S	Exibir informações do resumo de alarmes

Relatórios personalizados	S	S	S	S	S	Exibir relatórios de clientes
Publicação de painéis	-	S	-	-	S	Tornar os painéis publicados disponíveis
Relatórios de exibições dinâmicas	S	S	S	S	S	Visualizar relatórios de exibições dinâmicas
Relatórios unificados	S	S	-	-	S	Acesso aos relatórios unificados
Gráfico de detecção em pizza	-	S	-	-	S	Exibir informações de detecção
Painéis personalizados	S	S	S	S	S	Exibir painéis personalizados
Gerenciamento da detecção	-	S	-	-	S	Definir as propriedades do sistema do computador
Administração da conta	S	-	-	-	S	Gerenciar contatos de contas e personalizar o conteúdo do portal

Permissões	**Administrador**	**Criador de painéis**	**Hóspede**	**Operador**	**Superusuário**	**Descrição**
Monitoramento de usuários	S	-	-	-	S	Exibir e desconectar sessões de usuários
Gerador de relatórios	S	S	-	-	S	Criar, modificar e excluir relatórios
Painéis de exibições dinâmicas	S	S	-	S	S	Visualizar painéis de exibições dinâmicas
Criador de painéis	S	S	-	-	S	Criar, modificar e excluir painéis privados
Personalização padrão	S	-	-	-	S	Personalizar o conteúdo padrão do portal para usuários do Nimsoft

Personalização do usuário	S	S	S	S	S	Personalizar seu próprio conteúdo do portal
Alterar senha	S	S	-	S	S	O contato pode alterar sua própria senha
Administração do SLM	S	-	-	-	S	Executar o Gerenciador de nível de serviço com acesso completo
Acesso a SLO	S	S	-	S	S	Permitir que os usuários do portlet procurem dados do SLO
Acesso a QoS	S	S	-	S	S	Permitir que os usuários do portlet procurem séries de QoS
Exibição do SLM	S	S	-	S	S	Executar o Gerenciador de nível de serviço no modo somente leitura
Service Desk	S	S	-	S	S	Acessar os portlets Service Desk e Meus tickets
Editar modelos de monitoramento do USM	S	-	-	-	S	Criar, editar e excluir os modelos de monitoramento
Modificação de grupos do USM	S	-	-	-	S	Criar, editar e excluir grupos
Monitoramento de autoatendimento do USM	S	-	-	-	S	Ativar ou desativar os modelos de monitoramento prontos
USM básico	S	S	-	S	S	Acessar o portlet do USM

Instalação automática de robôs do USM	S	-	-	-	S	Implantar e instalar robôs automaticamente no sistema de destino
Modificar monitores individuais de sistemas de computador do USM	S	-	-	-	S	Criar, modificar e excluir monitores de SOC individuais
Visualizador de listas	S	S	-	S	S	Exibir listas e grupos
Criador de listas	S	S	-	-	S	Criar, modificar e excluir listas e grupos
Programador de relatórios	S	S	-	S	S	Acessar o portlet Agendador de relatórios
Netflow	S	S	-	-	S	Acessar o portlet NetFlow
Configuração do NetFlow	S	-	-	-	S	Permitir que os usuários do portlet definam as configurações do probe NetFlow
Serviço web	-	-	-	-	S	Acessar a API do serviço web do Nimsoft
Cloud UE Monitor	S	S	-	S	S	Acessar o portlet Cloud User Experience Monitor

Glossário

confirmar

Todas as novas mensagens de alarme recebidas pelo NAS (Nimsoft Alarm Server - Servidor de alarmes do Nimsoft) são inicialmente consideradas não confirmadas e apresentadas a um operador. Quando o operador tiver verificado e solucionado o problema, poderá confirmar a mensagem, indicando que o problema está sob controle. Em seguida, a mensagem é excluída do banco de dados do servidor de alarmes. Uma cópia é mantida no banco de dados de histórico.

níveis de alarme

Os níveis de alarme suportados são: limpar (0), informações (1), aviso (2), secundário (3), principal (4) e crítico (5).

mensagem de alarme

Um alarme é uma mensagem geral com o assunto definido como alarme. A mensagem é normalmente gerada por um probe respondendo a uma violação de limite e publicada como uma mensagem de alarme "bruta".

método de cálculo

Um método de cálculo é o conjunto de regras e condições que determinam a maneira como a conformidade com o SLA é calculada.

perfil de cálculo

Os perfis de cálculo são criados por usuários para definir as propriedades de cálculo dos objetos de nível de serviço e da qualidade de restrições do serviço. Os perfis se baseiam em plug-ins integrados distribuídos com o aplicativo Gerenciador de nível de serviço do Nimsoft. Os perfis são agrupados como cálculos de SLO ou cálculos de QoS, dependendo se o plugin selecionado oferece suporte a séries de dados únicas ou múltiplas.

percentual de conformidade

O percentual de conformidade é definido como a porcentagem de tempo em que a QoS, restrita por fatores como período operacional e limites, deve ser considerada compatível no período de conformidade.

período de conformidade

O período de conformidade define o período de tempo em que um SLA deve atender aos requisitos definidos pelo percentual de conformidade, geralmente um dia, uma semana ou um mês.

probe contínuo

Um probe contínuo está sempre ativo. Se for interrompido, o robô imediatamente tentará reiniciá-lo.

tipos de dados

Os tipos de dados usados para calcular a conformidade são Automático (intervalo), no qual os dados de QoS são gravados em intervalos, ou Assíncrono, no qual os dados de QoS somente são gravados cada vez que o valor medido é alterado.

domínio

Um *domínio* é um conjunto lógico no qual todos os componentes de infraestrutura são agrupados. Uma implantação geralmente tem um domínio. MSP ou implantações muito grandes podem usar domínios diferentes para cada empresa ou empreendimento.

histórico

Quando uma mensagem de alarme é confirmada ela é excluída do banco de dados do NAS, mas é mantida em um banco de dados de histórico. O conteúdo desse banco de dados pode ser exibido na janela de alarmes.

hub

O hub é um serviço na infraestrutura do Nimsoft que gerencia um grupo de robôs, coleta e redistribui as mensagens publicadas pelos probes, mantém vários serviços centrais e gerencia mensagens.

infraestrutura

Infraestrutura se refere ao domínio, hubs, robôs e probes do Nimsoft.

Infrastructure Manager

O Infrastructure Manager é a interface principal para a configuração e o gerenciamento do sistema Nimsoft. Ele fornece uma exibição hierárquica dos sistemas que estão sendo monitorados, uma janela de alarmes para exibir todos os alarmes e mensagens, e interfaces de configuração.

Endereço do Nimsoft

Um endereço do Nimsoft consiste em quatro elementos básicos, domínio, hub, robô e probe, cada um separado por uma barra. Por exemplo, em /Nimsoft /oslo /wscase /nas. A API do Nimsoft apresenta funções que resolvem um endereço do Nimsoft em um endereço IP ou porta.

período operacional

O período operacional restringe as amostras de QoS a uma ou mais especificações de tempo no período de conformidade. Isso significa que as amostras que ficarem fora dessas especificações de tempo não influenciarão os requisitos de conformidade com o SLO/SLA. Cada período operacional é definido como uma união de uma ou mais especificações de tempo.

probe

Um *probe* é um pequeno segmento de software que executa uma tarefa dedicada. **Probes de monitoramento**, coletam dados de desempenho e disponibilidade. **Probes de serviço** (também chamados de probes de utilitário), fornecem funções de utilitário do produto para a infraestrutura do Nimsoft. Os probes podem ser facilmente configurados para os seus próprios requisitos de monitoramento específicos.

mensagem publicada

Uma mensagem é publicada quando é enviada ao hub mais próximo, sem ser destinada a um destinatário específico. Em seguida, a mensagem pode ser entregue a todos os clientes com assinatura para a ID do assunto encontrado na mensagem.

QoS (Qualidade de Serviço)

A QoS é o valor real coletado por um probe e usado de forma centralizada para determinar o estado do objetivo do nível de serviço. Se o probe estiver configurado para fornecer Qualidade de serviço, uma mensagem de QoS será emitida. Esse valor é usado para alarmes.

mensagens de qualidade de serviço (QoS)

As mensagens de qualidade de serviço fornecem dados de tendências periodicamente. Elas normalmente contêm dados (como tempo de resposta e disponibilidade) usados para o monitoramento e para a geração de relatórios do nível de serviço.

robô

O robô é a primeira linha de gerenciamento para os probes. O robô inicia e interrompe os probes nos horários requeridos, e coleta, enfileira e encaminha mensagens dos probes para o hub.

SLA (Service Level Agreement - Acordo de nível de serviço)

Um SLA é um acordo para fornecer um serviço dentro de um período de tempo fixo/especificado. Ambas as partes (por exemplo, um departamento de TI que fornece serviços para outro departamento ou uma empresa e um fornecedor de serviços externos) concordam com os níveis mensuráveis de serviço.

SID (Subject ID - ID do assunto)

Uma ID do assunto é uma sequência de caracteres de texto que classifica as mensagens do Nimsoft e torna possível que os clientes assinem algumas mensagens e ignorem outras. Todas as mensagens com o mesmo assunto devem também ter estrutura de dados idêntica.

assinar

Um cliente (por exemplo, um probe ou gateway) pode assinar mensagens com base na ID do assunto. Isso permite que ele receba todas as mensagens semelhantes (por exemplo, alarmes).

ID do subsistema

A ID do subsistema é um campo em todas as mensagens de alarme que contém um ou mais números separados por pontos, por exemplo, 2.31.4. A ID do subsistema corresponde aos módulos do sistema monitorado, como sistemas de segurança ou de discos. O Console de alarmes agrupa os alarmes de entrada de acordo com o subsistema, permitindo a rápida exibição de todos os alarmes para uma determinada área.

supressão

A supressão trata diversos alarmes idênticos como uma única mensagem. Algumas vezes, os probes de alarme do Nimsoft geram uma série de alarmes idênticos. Ativar a supressão reduz a quantidade de mensagens desnecessárias apresentadas ao operador.

probe programado

Um probe programado faz a execução uma vez e termina, aguardando o próximo ponto no período em que está configurado para iniciar.