Relatório Estudo Dirigido SNMP - Redes de Computadores

Matheus Baron Lauritzen[1], Gustavo Baron Lauritzen[1]

[1]Escola Politécnica – Ciência da Computação – Universidade do Vale do Itajai (UNIVALI)
Itajaí – Santa Catarina – SC – Brasil

Parte 01 - Estudo do SNMP

Perguntas Teóricas:

Explique a função do SNMP no contexto do gerenciamento de redes.

O SNMP (Simple Network Management Protocol) é um protocolo de camada de aplicação que facilita a troca de informações de gerenciamento entre dispositivos de rede. Sua função principal é permitir que administradores de rede monitorem o desempenho da rede, identifiquem e diagnostiquem problemas, e configurem dispositivos remotamente. Ele atua coletando dados de dispositivos como roteadores, switches, servidores e impressoras, tornando o gerenciamento de infraestruturas de rede complexas mais eficiente. **Diferencie os papéis do gerente e do agente SNMP.**

No SNMP, existem dois papéis principais:

2.
- **Gerente (Manager):** É a estação de gerenciamento, um software ou aplicação que roda em um computador, responsável por monitorar e controlar os dispositivos de rede. Ele envia requisições (como Get, GetNext, GetBulk, Set) para os agentes e recebe as respostas e as notificações (Traps e InformRequests) dos agentes.
- **Agente (Agent):** É um software que roda nos dispositivos de rede (e.g., roteadores, switches, servidores). Ele coleta informações sobre o dispositivo (CPU, memória, tráfego de rede, etc.), armazena-as em uma MIB (Management Information Base) e responde às requisições do gerente. O agente também pode enviar notificações proativas (Traps ou InformRequests) ao gerente em caso de eventos significativos.

3. **O que é uma MIB e qual a sua importância no SNMP?**

   Uma MIB (Management Information Base) é uma base de dados hierárquica e formalmente definida que descreve a estrutura das informações de gerenciamento para dispositivos em uma rede. Em termos mais simples, é um dicionário padronizado de objetos que podem ser gerenciados. Cada objeto na MIB possui um OID (Object Identifier) único.

   Importância: A MIB é crucial porque padroniza como os dados de gerenciamento são organizados e acessados. Ela garante que diferentes dispositivos de diferentes fabricantes possam ser gerenciados usando o mesmo protocolo SNMP, pois todos entendem a mesma linguagem de dados definida na MIB. Sem a MIB, o gerente não saberia quais dados coletar ou como interpretá-los de forma consistente.

4. **Compare as versões SNMPv1, SNMPv2c e SNMPv3 quanto a funcionalidade**

Segurança: Permanece a mesma do SNMPv1, utilizando ”community strings”em texto claro. A letra ”c”em v2c indica que ainda é baseado em comunidade e, portanto, sem segurança aprimorada.

- **SNMPv3:**

  Funcionalidade: Mantém as funcionalidades do SNMPv2c, mas foca drasticamente nas melhorias de segurança. Introduz modelos de segurança e modelos de visão de dados. **Segurança:** Representa um avanço significativo. Oferece:

  - * **Autenticação:** Garante que as mensagens vêm de uma fonte autorizada, usando algoritmos como MD5 ou SHA.
    * **Privacidade (Criptografia):** Protege a confidencialidade dos dados, impedindo que terceiros leiam as informações (e.g., com DES ou AES).
    * **Integridade:** Garante que a mensagem não foi alterada em trânsito.

  É a versão mais recomendada e utilizada em ambientes de produção que exigem segurança.

5. **Quais são os principais tipos de mensagens utilizadas no SNMP?**

   Os principais tipos de mensagens (PDUs - Protocol Data Units) utilizadas no SNMP são:

   GetRequest: Enviado pelo gerente para um agente para recuperar o valor de uma ou mais variáveis de MIB específicas. **GetNextRequest:** Enviado pelo gerente para um agente para recuperar o valor da próxima variável de MIB na ordem lexicográfica. Usado para ”caminhar”(walk) por tabelas de MIB. **GetBulkRequest (SNMPv2c/v3):** Enviado pelo gerente para um agente para recuperar um grande bloco de dados de forma eficiente, minimizando o número de requisições. **GetResponse:** Enviado pelo agente em resposta a um GetRequest, GetNextRequest, GetBulkRequest ou SetRequest, contendo os valores solicitados ou um erro. **SetRequest:** Enviado pelo gerente para um agente para modificar o valor de uma ou mais variáveis de MIB (para configurar o dispositivo). **Trap:** Enviado de forma assíncrona pelo agente para o gerente para notificar sobre um evento significativo que ocorreu (e.g., porta down, falha de hardware). Não requer confirmação do gerente no SNMPv1/v2c. **InformRequest (SNMPv2c/v3):** Semelhante a um Trap, mas exige que o gerente envie um GetResponse de volta para confirmar o recebimento. Isso garante maior confiabilidade na entrega da notificação.

6. **Por que o SNMP é considerado independente da tecnologia de rede subjacente?**

O SNMP é considerado independente da tecnologia de rede subjacente porque ele opera na camada de aplicação (Camada 7 do modelo OSI) e, como tal, utiliza serviços de transporte comuns como UDP (User Datagram Protocol) ou TCP (Transmission Control Protocol), que por sua vez podem ser encapsulados por qualquer tecnologia de camada de rede ou enlace de dados.

Isso significa que o SNMP não se importa se a rede está usando Ethernet, Wi-Fi, Token Ring, Frame Relay, ATM, MPLS ou qualquer outra tecnologia de camada 2 ou 3. Enquanto houver conectividade IP (Internet Protocol) entre o gerente e o agente, o SNMP pode funcionar. Essa característica o torna extremamente versátil e amplamente aplicável em diversos tipos de ambientes de rede.

1. Introdução

Este relatório detalha a implementação prática de monitoramento de rede utilizando o protocolo SNMPv2, conforme proposto no estudo dirigido. O objetivo foi configurar um ambiente com um Zabbix Server para monitorar um Agente SNMP em uma máquina virtual, compreendendo a arquitetura, o fluxo de comunicação e os desafios práticos da configuração.

2. Arquitetura do Ambiente

O laboratório foi montado com os seguintes componentes:

- **Zabbix Server (Gerente SNMP):**
  - Sistema Operacional: Ubuntu 24.04 LTS (Máquina Física)
  - IP: 192.168.1.11
  - Software: Zabbix Server, Zabbix Frontend (Apache), MariaDB.
- **SNMP Agent (Agente SNMP):**
  - Sistema Operacional: Ubuntu 24.04 LTS (Máquina Virtual no VirtualBox)
  - IP: 192.168.1.12
  - Software: snmpd (Net-SNMP).

O fluxo de comunicação se deu com o Zabbix Server (Gerente) enviando requisições SNMP (get-request) para o Agente na VM pela porta UDP 161. O Agente, por sua vez, respondia com os dados solicitados (get-response).

3. Desafios Encontrados e Soluções

A configuração do ambiente apresentou diversos desafios que foram cruciais para o aprendizado:

- **Erro de Resolução de MIBs:**
  - Sintoma: O comando snmpwalk falhava com o erro `system: Unknown Object Identifier`.
  - Causa: A configuração padrão do cliente SNMP no Ubuntu (`/etc/snmp/snmp.conf`) desabilita o carregamento de MIBs com a linha `mibs :`.
  - Solução: Foi necessário instalar o pacote `snmp-mibs-downloader` e comentar a linha `mibs :` nos arquivos de configuração tanto da VM (Agente) quanto da máquina física (Servidor) para permitir a tradução dos OIDs.

- **Timeout de Rede:**
  - Sintoma: O snmpwalk do servidor para a VM resultava em `Timeout: No Response`.
  - Causa: A configuração de rede da VM no VirtualBox estava em modo ”NAT”, que impede conexões iniciadas de fora para dentro da VM.
  - Solução: A rede da VM foi alterada para o modo ”Placa em modo Bridge”, o que a colocou na mesma rede local do servidor e permitiu a comunicação direta.
- **Aviso ”Zabbix server is not running”:**
  - Sintoma: O frontend do Zabbix exibia um aviso de que o servidor não estava rodando, impedindo a coleta de dados.
  - Causa: O processo do Zabbix Server não conseguia se conectar ao banco de dados MariaDB devido à falta da senha no arquivo de configuração (`/etc/zabbix/zabbix_server.conf`). A linha `DBPassword` estava comentada.
  - Solução: A linha `DBPassword` foi descomentada e preenchida com a senha correta do banco de dados, permitindo que o servidor se conectasse e iniciasse completamente.

4. Análise de Tráfego com Wireshark

Para validar a comunicação, o tráfego entre o Zabbix Server e o Agente foi capturado com o Wireshark. O filtro `snmp` foi aplicado para isolar os pacotes relevantes.

- **Exemplo de Requisição (GET-REQUEST):**
  - Origem: [IP do seu Zabbix Server]
  - Destino: 192.168.1.12
  - Protocolo: SNMP
  - Informação: get-request 1.3.6.1.2.1.1.1.0 (sysDescr.0)
  - Análise: O Zabbix Server solicita a descrição do sistema (OID 1.3.6.1.2.1.1.1.0).
  - Dados do Wireshark:

```
79612 1033.997780500
192.168.1.11 192.168.1.12 SNMP 122 get-request
1.3.6.1.4.1.2021.10.1.3.3 1.3.6.1.4.1.2021.10.1.3.2 1.3.6.1.4
```

- **Exemplo de Resposta (GET-RESPONSE):**
  - Origem: 192.168.1.12
  - Destino: [IP do seu Zabbix Server]
  - Protocolo: SNMP
  - Informação: get-response 1.3.6.1.2.1.1.1.0
  - Análise: O Agente SNMP responde com o valor solicitado: ”Linux ubuntu-snmp-VirtualBox...”
  - Dados do Wireshark:

```
799801064.029868223
192.168.1.12 192.168.1.11 SNMP 106
get-response
1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.25.1.1.0
```

5. Conclusão

O estudo dirigido foi concluído com sucesso. Foi possível configurar um ambiente de monitoramento SNMP funcional, superando desafios práticos de configuração de rede, software e segurança. A análise com o Wireshark confirmou o correto funcionamento do protocolo, validando a troca de requisições e respostas entre o gerente e o agente. O conhecimento adquirido sobre o diagnóstico de problemas foi o maior ganho da atividade.

Parte 03 - Atividades de Aprofundamento

Analise a diferença entre usar o protocolo SNMP e o Zabbix Agent para monitoramento. Embora tanto o SNMP quanto o Zabbix Agent sirvam para coletar dados de monitoramento de dispositivos, eles operam de maneiras distintas e possuem diferentes características:

1. • **Protocolo SNMP:**

   Padrão Aberto: É um protocolo padrão da indústria, amplamente suportado por praticamente todos os fabricantes de hardware de rede (roteadores, switches, impressoras, etc.) e muitos sistemas operacionais. Isso o torna ideal para monitoramento heterogêneo. **Leitura de MIBs:** Opera lendo e, ocasionalmente, escrevendo em MIBs (Management Information Bases) padronizadas ou proprietárias, que definem os dados que podem ser coletados. **Modo de Operação:** Funciona primariamente no modelo ”pull”(gerente solicita dados) com a capacidade de ”push”para eventos críticos (Traps e InformRequests). **Segurança:** As versões mais antigas (v1, v2c) têm segurança limitada (community strings em texto claro). O SNMPv3 oferece autenticação e criptografia, mas é mais complexo de configurar. **Dados Coletados:** Geralmente focado em métricas de hardware (status de interface, uso de CPU/memória de dispositivo de rede, etc.) e informações de sistema operacional mais genéricas. Pode ser limitado na granularidade e em dados específicos de aplicações.

- **Zabbix Agent:**

  Específico da Ferramenta: É um software proprietário do Zabbix, otimizado para coletar dados de hosts onde ele é instalado (servidores, máquinas virtuais). Não é um padrão aberto para comunicação de rede geral. **Flexibilidade Alta:** Permite a coleta de uma gama muito mais ampla de dados, incluindo métricas de sistema operacional (uso de disco, processos, logs), performance de aplicações (web servers, bancos de dados), e execução de scripts personalizados. **Modo de Operação:** Suporta tanto o modelo ”pull”(server/proxy solicita dados) quanto o ”push”(agent envia Trappers para o server/proxy). **Segurança:** As comunicações entre o Zabbix Server/Proxy e o Agent podem ser criptografadas (PSK ou certificados), oferecendo um nível de segurança robusto. **Dados Coletados:** Ideal

para monitoramento detalhado de servidores e aplicações, oferecendo alta granularidade e a capacidade de coletar métricas muito específicas que não seriam expostas via SNMP.

- **Conclusão:** O SNMP é excelente para monitorar a infraestrutura de rede (roteadores, switches) e dispositivos onde não é possível instalar um agente (impressoras, alguns dispositivos IoT). O Zabbix Agent é a escolha preferencial para monitoramento aprofundado de servidores, VMs e aplicações, onde a granularidade, a flexibilidade de coleta e a segurança são críticas. Em um ambiente real, ambos são frequentemente usados em conjunto para cobrir todas as necessidades de monitoramento.

Diagrama da Arquitetura (Código Mermaid)

A arquitetura do ambiente de monitoramento com Zabbix e SNMP pode ser visualizada através do seguinte código Mermaid. Este código pode ser renderizado em ferramentas que suportam Mermaid para gerar um diagrama visual.

Listing 1. Código Mermaid do Diagrama da Arquitetura de Monitoramento com Zabbix e SNMP

```
graph TD
    subgraph "Máquina Física (c-3po - Zabbix Server)"
        Admin["Administrador (Você)"]
        Frontend[Zabbix Frontend (Web)]
        Server[Zabbix Server (Processo)]
        DB[(MariaDB)]

        Admin -- "Acessa via<br>Navegador (HTTP)" --> Frontend
        Frontend -- "L /Escreve Dados de Config." --> DB
        Server -- "Armazena/L Dados Coletados" --> DB
    end

    subgraph "Máquina Virtual (ubuntu-snmp-VirtualBox - Agente)"
        Agent[Agente SNMP (snmpd)]
        OS[Recursos do SO<br>CPU, Memória, Rede]

        Agent -- "L Métricas Locais" --> OS
    end

    Server -- "SNMP GET<br>(UDP Porta 161)" --> Agent
    Agent -- "SNMP RESPONSE" --> Server
```

Explicação da Arquitetura

Componentes:

- **Administrador (Você):** O usuário final que gerencia o sistema, visualiza os dados e configura o monitoramento através da interface web.
- **Zabbix Frontend (Web):** A interface gráfica acessada pelo navegador. É servida pelo Apache e se comunica com o banco de dados para ler e escrever configurações (hosts, templates, etc.) e exibir os dados coletados.

- **Zabbix Server (Processo):** O ”cérebro”do Zabbix. É o processo de backend que realiza o monitoramento ativo. Ele sabe quais hosts monitorar, quais itens coletar e quando. É ele quem atua como Gerente SNMP, enviando as requisições.
- **MariaDB (Banco de Dados):** O repositório onde todas as informações são armazenadas, incluindo as configurações de hosts, os dados históricos coletados e as informações dos usuários.
- **Agente SNMP (snmpd):** O processo que roda na máquina virtual monitorada. Ele tem acesso às informações e métricas do sistema operacional e aguarda por requisições do Gerente SNMP na porta UDP 161.
- **Recursos do SO:** Representa o próprio sistema operacional da VM, de onde o Agente SNMP coleta os dados (uso de CPU, memória disponível, tráfego de rede, etc.).

Fluxo de Dados:

(a) O Administrador acessa o Zabbix Frontend para configurar o monitoramento do host 192.168.1.12.
(b) O Zabbix Server (Gerente SNMP), seguindo a configuração, envia uma requisição SNMP GET para o Agente SNMP na VM, através da porta UDP 161.
(c) O Agente SNMP recebe a requisição, coleta a informação solicitada dos Recursos do SO (por exemplo, a carga da CPU).
(d) O Agente envia a informação de volta para o Zabbix Server em um pacote SNMP RESPONSE.
(e) O Zabbix Server recebe a resposta e armazena o valor (a carga da CPU) no banco de dados MariaDB, associado ao host e ao item correto.
(f) Quando o Administrador visualiza os ”Latest data”no Frontend, a interface web lê essa informação diretamente do MariaDB para exibi-la.

Atividades de Aprofundamento: Criação de Alertas SNMP Personalizados

Para demonstrar a capacidade de monitoramento proativo e a criação de alertas baseados em OIDs SNMP específicos, foi configurado um acionador (trigger) no Zabbix para alertar quando o tempo de atividade da VM excedesse 5 minutos.

Identificação do OID Personalizado

O primeiro passo foi identificar o OID (Object Identifier) correspondente ao tempo de atividade do sistema (System Uptime). Utilizando o comando `snmpwalk` na máquina física, foi possível obter o OID e o formato do valor retornado:

Comando Executado:

Listing 2. Comando snmpwalk para System Uptime

```
snmpwalk -v2c -c public 192.168.1.12 1.3.6.1.2.1.1.3.0
```

Saída Esperada:

Listing 3. Exemplo de Saída do snmpwalk para System Uptime

```
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (XXXXX) HH:MM:SS.
```

O OID identificado foi `1.3.6.1.2.1.1.3.0`, e o valor é retornado em "timeticks"(centésimos de segundo).

Criação do Item no Zabbix

Um novo item foi criado no Zabbix para coletar o valor do OID `1.3.6.1.2.1.1.3.0` da VM, com as seguintes configurações:

- **Nome do Item:** Tempo de Atividade do Sistema
- **Tipo:** Agente SNMP
- **Chave:** `tempo.atividade.snmp`
- **OID SNMP:** `1.3.6.1.2.1.1.3.0`
- **Tipo de informação:** Numérico (não assinado)
- **Intervalo de atualização:** 30s

Criação do Acionador (Trigger)

Um acionador foi configurado para disparar um alerta quando o valor do item "Tempo de Atividade do Sistema"excedesse 5 minutos (300 segundos, ou 30.000 timeticks), com as seguintes propriedades:

- **Nome do Acionador:** VM ligada por mais de 5 minutos
- **Severidade:** Aviso
- **Expressão:**

Listing 4. Expressão da Trigger para Tempo de Atividade

```
last(/SNMP-Agent-1/tempo.atividade.snmp)>30000
```

Esta expressão verifica se o último valor coletado para o item `tempo.atividade.snmp` do host `SNMP-Agent-1` é maior que 30.000 timeticks.

Verificação do Alerta

Após a configuração, o alerta foi visualizado na seção **Monitoramento** $\rightarrow$ **Problemas** do frontend do Zabbix, confirmando o disparo do acionador quando a condição de tempo de atividade foi atendida.