INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

105 ANOS
REDE FEDERAL
DE EDUCAÇÃO
PROFISSIONAL
E TECNOLÓGICA
1909-2014

Gerência de Redes

Turma : 20172.5.01405.1N

SNMPv3

Prof. Thiago Dutra <thiago.dutra@ifrn.edu.br>

Agenda

- Histórico
- Introdução
- Entidades SNMP
  - Mecanismo SNMPv3
  - Aplicações SNMPv3
  - Convenções de Texto SNMPv3
- Segurança
  - USM
  - VACM
- SNMPv3 na prática

Histórico

- Grupo de trabalho do IETF criado em março de 1997
- Em Janeiro de 1998 vários documentos já tinham sido produzidos
- Em Abril de 1999 os documentos principais foram atualizados, são eles:
  - RFC 2571 → An architecture for describing SNMP management framework
  - RFC 2572 → Message processing and dispatching for SNMP
  - RFC 2573 → SNMPv3 applications
  - RFC 2574 → User based security model (USM) for SNMPv3
  - RFC 2575 → View based access control model (VACM) for SNMP

3

Introdução

- O SNMPv2 trouxe uma série de melhorias ao protocolo SNMP, entretanto manteve os mesmos problemas de segurança existentes no SNMPv1
- O SNMPv3, de fato, não define uma nova versão do protocolo SNMP, mas sim, um novo "framework" de gerenciamento e um conjunto de "security capabilities" que podem ser utilizadas pelo SNMPv1 e SNMPv2

4

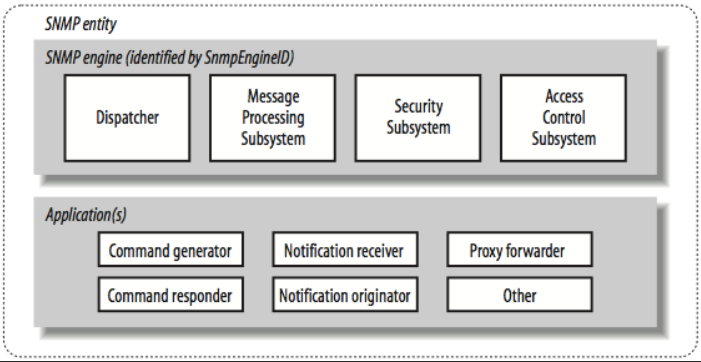
Introdução

- O SNMPv3 define uma ”arquitetura” para o SNMP, onde um dos elementos existentes é a segurança
- Nenhuma nova operação foi criada com o SNMPv3
  - A mensagens SNMPv1 e SNMPv2 continuam sendo utilizadas
- O cabeçalho da mensagem SNMP passa a conter informações relacionadas à segurança da mesma
- ”SNMPv3 is SNMPv2 plus security and administration”

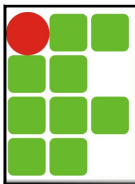
5

Entidades SNMP

- A alteração mais importante trazida pelo SNMPv3 reside no fato do abandono à ideia de gerentes e agentes
- Passa a existir apenas a figura da Entidade SNMP



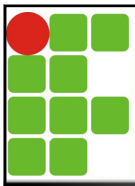
6



Mecanismo SNMPv3

- O mecanismo SNMPv3 é formado por quatro componentes:
  - Dispatcher (Escalonador)
  - Message Processing Subsystem (Subsistema de processamento de mensagens)
  - Security Subsystem (Subsistema de segurança)
  - Access Control Subsystem (Subsistema de controle de acesso)

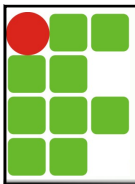
7



Mecanismo SNMPv3

- Dispatcher
  - Responsável por enviar e receber as mensagens
  - Tenta detectar a versão de cada mensagem e, se a versão for aceita, direcionada a mensagem para o Message Processing Subsystem
  - Também responsável por enviar mensagens SNMP para outras entidades

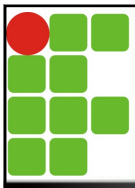
8



Mecanismo SNMPv3

- Message Processing Subsystem
  - Prepara as mensagens para serem enviadas
  - Recupera os dados das mensagens recebidas
  - Pode conter diversos módulos de processamento de mensagens
    - Ex.: Módulos para processar solicitações SNMPv1, SNMPv2, SNMPv3 e para outro modelo ainda não definido

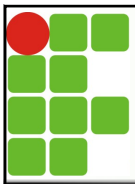
9



Mecanismo SNMPv3

- Security Subsystem
  - Oferece recursos de autenticação e serviços de privacidade
  - A autenticação usa strings de comunidade (para SNMPv1 e SNMPv2) ou autenticação baseada em usuário no SNMPv3
    - A autenticação baseada em usuário utiliza algoritmos MD5 ou SHA
  - Os serviços de privacidade usam por padrão o algoritmo DES para criptografar (codificar e decodificar) mensagens do SNMP
    - É possível a utilização de outros algoritmos

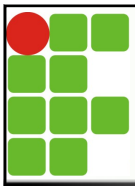
10



Mecanismo SNMPv3

- Access Control Subsystem
  - Responde pelo controle de acesso aos objetos da MIB
  - Permite controlar os objetos que o usuário pode acessar e as operações que executará nesses objetos
    - Ex.: permitir o acesso read-write de um usuário a algumas partes da árvore mib-2, e permitir o acesso somente leitura à árvore inteira

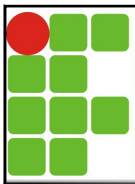
11



Aplicações SNMPv3

- Uma entidade pode ter até seis aplicações SNMPv3:
  - Command Generator (Gerador de comandos)
  - Command Responder (Replicador de comandos)
  - Notification Originator (Gerador de notificações)
  - Notification Receiver (Receptor de notificações)
  - Proxy Forwarder (Direcionador proxy)
  - Other (Outros)

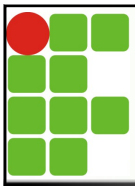
12



Aplicações SNMPv3

- Command Generator
  - Gera solicitações de get, get-next, get-bulk e set
  - Processa as respostas
  - Aplicação implementada por uma NMS (Network Managment Station)
- Command Responder
  - Responde às solicitações dos comandos get, get-next, get-bulk e set
  - No SMPV3 essa aplicação é implementada por uma entidade; no SNMPv1 e SNPMv2 é implementada pelo agente

13



Aplicações SNMPv3

- Notification Originator
  - Gera TRAPs e notificações do SNMP
  - No SMPV3 essa aplicação é implementada por uma entidade; no SNMPv1 e SNPMv2 é parte integrante do agente ou de algum utilitário
- Notification Receiver
  - Recebe traps e mensagens informativas
  - Aplicação implementada por uma NMS (Network Managment Station)

14

Aplicações SNMPv3

- Proxy Forwarder
  - Facilitador da transmissão de mensagens entre entidades
- Other
  - A RFC 2571 possibilitou que aplicações adicionais sejam definidas
  - Essa possibilidade de extensão da estrutura do SNMPv3 é uma vantagem significativa em relação as versões anteriores

15

Convenções de Texto SNMPv3

Textual convention	Description
snmpEngineID	An administratively unique identifier for an SNMP engine. Objects of this type are for identification, not for addressing, even though an address can be used in the generation of a specific value. RFC 3411 provides a detailed discussion of how snmpEngineIDs are created.
snmpSecurityModel	An SNMP securityModel (SNMPv1, SNMPv2, or USM). USM stands for User-based Security Model, which is the security method used in SNMPv3.
snmpMessageProcessingModel	A message processing model used by the Message Processing Subsystem.
snmpSecurityLevel	The level of security at which SNMP messages can be sent, or the level of security at which operations are being processed. Possible values are noAuthNoPriv (without authentication and without privacy), authNoPriv (with authentication but without privacy), and authPriv (with authentication and with privacy). These three values are ordered such that noAuthNoPriv is less than authNoPriv and authNoPriv is less than authPriv.
snmpAdminString	An octet string containing administrative information, preferably in human-readable form. The string can be up to 255 bytes long.
snmpTagValue	An octet string containing a tag value. Tag values are preferably in human-readable form. According to RFC 3413, valid example tags include acme, router, and host.
snmpTagList	An octet string containing a list of tag values. Tag values are preferably in human-readable form. According to RFC 3413, valid examples of a tag list are the empty string, acme router, and host managerStation.
KeyChange	An object used to change authentication and privacy keys.

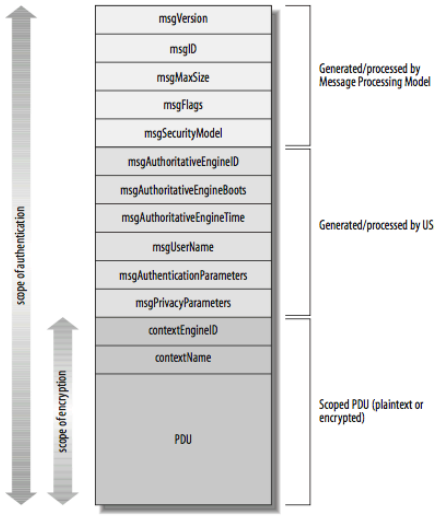
16

Segurança

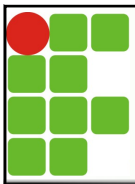
- As melhorias relacionadas a segurança do protocolo SNMP são fornecidas através da junção do USM (User-based Security Model) e VACM (View Access Control Model)
- Essas melhorias são implementadas com a extensão do cabeçalho
  - Uma série de informações sobre os mecanismos de segurança em uso foram inseridas no cabeçalho
  - As PDUs SNMP continuam sendo as mesmas definidas no SNMPv1 e SNMPv2

17

Segurança



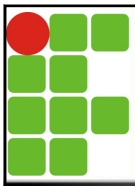
18



USM

- USM
  - Definido na RFC 2574, sua especificação engloba:
    - Autenticação: Possibilita a comprovação da integridade bem como da origem de uma mensagem. Utiliza o algoritmo HMAC e as funções de hash MD5 ou SHA1
    - Privacidade: Possibilita a cifragem da mensagem, utilizando o algoritmo DES
    - Timeliness: Protege contra ataques de ”replay” e ”delay”

19



USM

- USM
  - Definido na RFC 2574, sua especificação engloba:
    - Formato de mensagem: Define os campos a serem inseridos no cabeçalho da mensagem SNMPv3, logo após um MsgSecurityModel=3
    - Descoberta: Define procedimentos através dos quais uma entidade SNMP pode obter informações sobre outra
    - Gerenciamento de chaves: Define procedimentos para a geração, uso e atualização de chaves

20

VACM

- VACM
  - Definido na RFC 2575, determina se o acesso a um objeto de uma MIB local deve ser permitido
  - O VACM utiliza uma MIB que define a política de controle de acesso para a entidade
  - Na sua definição estão presentes cinco elementos: Grupos; Níveis de Segurança; Contextos; Visões de MIBs e Políticas de Acesso

21

VACM

- Grupos
  - É uma ferramenta utilizada para categorizar entidades, com respeito aos direitos de acesso
  - Por exemplo, todos as entidades de mais alto nível podem ter um mesmo conjunto de direitos de acesso, diferente do possuído por entidades de nível intermediário
- Níveis de Segurança
  - São aplicados a cada grupo e relacionados ao nível de segurança das mensagens recebidas
  - Por exemplo, uma entidade pode restringir o acesso ao modo "somente leitura" caso a mensagem recebida não esteja autenticada
    - Uma requisição idêntica vinda com código de autenticação, passaria a ter direito de escrita

22

VACM

- Contexto e Visões de MIB
  - Um contexto é definido como um subconjunto de objetos da MIB de uma entidade ao qual se atribui um nome
    - Conceito semelhante as views do SNMPv2
  - Os privilégios de controle de acesso entre as entidades são expressos na forma de
    - Um usuário configurado na entidade
    - Uma visão da MIB "criada" em um contexto e aplicada a este usuário

23

VACM

- Políticas de Acesso
  - Um agente SNMP pode ser configurado para impor um conjunto particular de direitos de acesso com base no:
    - Usuário que está realizando a requisição
    - Nível de segurança da mensagem de requisição
    - Security model da mensagem de requisição
    - Contexto da MIB acessado na requisição
    - Objeto específico que foi requisitado
    - Tipo de acesso requisitado (leitura, escrita)

24

SNMPv3 na prática

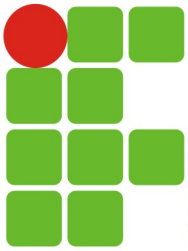
- O que, normalmente, é configurado num dispositivo para utilizar o SNMPv3?
  - Username
  - Security Level
    - Ex.: noAuthNoPriv, authNoPriv e authPriv
  - Authentication: protocol e passphrase
  - Privacy: protocol e passphrase
- Passos lógicos para uso do SNMPv3
  - 1 – Criar uma entrada USM, com os devidos atributos, no dispositivo a ser gerenciado
  - 2 – Configurar a estão de gerenciamento com os atributos apropriados para o dispositivo gerenciado
  - 3 – Começar a gerenciar o dispositivo

25

Referências

- MAURO, Douglas R., SHCMIDT, Kevin J. – **SNMP Essencial**. 1ª Ed., Editora Campus, 2001.
- MAURO, Douglas R., SHCMIDT, Kevin J. – **Essential SNMP**. 2ª Ed., Editora O`Reilly, 2005.
- NETWORK WORKING GROUP. – **RFCs 2571 a 2575**. disponível em:
  - https://www.ietf.org/rfc/rfc2571.txt
  - https://www.ietf.org/rfc/rfc2572.txt
  - https://www.ietf.org/rfc/rfc2573.txt
  - https://www.ietf.org/rfc/rfc2574.txt
  - https://www.ietf.org/rfc/rfc2575.txt

26



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Gerência de Redes

Turma : 20172.5.01405.1N

SNMPv3

Prof. Thiago Dutra <thiago.dutra@ifrn.edu.br>