Course ID
SNMPV3

Course Title
SNMPv3: Secure SNMP

Course Duration
1 day

Related Courses

- SNMP: Agent Development (1 day, SNMP-AGENT)

Aimed At

IT professionals, engineers, tech and customer support representatives, marketing and sales personnel and others responsible for SNMP deployment and management, agent development, and SNMP sales and support.

Group Size

5-25

Prerequisites

- SNMP Essentials: A Fast-Track Tutorial (3 days, SNMP-ESSENT)

Course in a Nutshell

SNMPv1 and SNMPv2c both provide "community string" security, also called "Trivial Authentication". SNMPv3 offers significant improvements. The SNMPv3 architecture incorporates new descriptions for SNMP Entities (Managers, Agents, Proxy Forwarders), updated message formats, and Standard MIBs used to configure access to Entities. New features include: User authentication using entity shared secret keys, along with message time stamps; data secrecy using encryption; and control of user access to MIB information based on the need to know.

SNMPv3 messages can be sent at any of the following three levels of security:

- No Authentication and No Encryption. Also called "noAuth/noPriv", "Priv" referring to Privacy. Only a valid User Name is required to access data or to send a trap.
- Authentication and No Encryption, also called "Auth/noPriv". The User must be authenticated as a valid user for the message to be accepted. This is accomplished by sharing a secret key, and using that key to produce a message hashed authentication code sent with each message.
- Authentication and Encryption, also called "Auth/Priv". The User is authenticated and the data payload is encrypted using a second shared secret key.

SNMPv3's View Access Control Model (VACM) is used to control access to specific MIB data. Individual users are configured into groups, and groups might have the following privileges. Only Security Administrators can access the MIB data to configure SNMPv3 MIBs at remotely managed agents. Microwave Engineers can control remote microwave radios, including the ability to reboot them if necessary. The report generator group can access appropriate read-only data as needed.

This intensive, one-day tutorial, the second of out three-course series on SNMP, outlines the new message formats, the SNMPv3 configuration MIBs and related RFC's, and describes the relationships. It will help you understand the threats addressed by SNMPv3, and the methods used to counter those threats.

Learn How To

- Explain the threats addressed by SNMPv3.
- Define the new SNMPv3 terminology.
- Describe the new SNMPv3 message structures.
- Configure Managers, Agents, and Proxy Forwarders for SNMPv3, and to also be able to communicate in SNMPv1 & SNMPv2c environments.

Course Outline

- Threats Addressed by SNMPv3
- Relationship of SNMPv3 to SNMPv1 and SNMPv2c
- SNMPv3 Architecture Descriptions
- SNMPv3 Messages
  - Contents and structure
  - Relationships to the SNMPv3 security models
- Security Details
  - User-Based Security Model (USM)
    - Users, groups, and security models
  - Message authentication and authentication keys
  - PDU (Protocol Data Unit) encryption
  - View-based Access Model (VACM)
  - Message timeliness checks
  - Security options
- Configuration
  - SNMPv3 Configuration MIB Tables
  - Manager configuration
  - Agent configuration
  - Configuration to support SNMPv1 & SNMPv2c messaging
  - Proxy forwarders
  - Examples
- Wrap-up: Course Recap, Q/A, and Evaluations

How You Will Learn

- You will learn in interactive lecture/workshop format from an instructor who's an expert practitioner and teacher of SNMP.
- Along with lecture, we will use interaction and activities to enrich the instruction and drive home the essential points.
- The course materials are designed to be an instructional aid as well as a lasting professional reference.

Revised *February 16, 2007*

Website: www.eogogics.com
E-mail: sales@eogogics.com
Tel. +1 (703) 281-3525
Fax +1 (866) 612-6896