Elementy architektury zarządzania siecią w SNMP

- stacja zarządzająca
- agent zarządzający
- baza informacji
- protokół zarządzania siecią

Stacja zarządzająca powinna być wyposażona w następujące elementy:

- zestaw aplikacji służących do analizy informacji, naprawiania błędów itp.
- interfejs służacy administratorowi do obserwacji i kontroli sieci

Elementy architektury zarządzanie siecią w SNMP cd.

- możliwość przekładania wymagań administratora sieci na faktyczną możliwość obserwacji i kontroli elementów sieci
- bazę danych zawierającą informacje z baz informacji administracyjnych (MIB) wszystkich jednostek w administrowanej sieci

Polecenia SNMP

- GetRequest - dla każdego obiektu wymienionego w poleceniu zwróć wartość tego obiektu
- GetNextRequest - dla każdego obiektu wymienionego w poleceniu zwróć wartość następnego obiektu (w porządku leksykograficznym danego MIBa)
- GetBulk (SNMPv2) - dla każdego obiektu wymienionego w poleceniu zwróć wartość następnych N obiektów
- SetRequest - dla każdego obiektu wymienionego w poleceniu ustaw wartość na wymienioną w poleceniu
- Trap - prześlij informację o zaistniałym zdarzeniu (agent do menedżera)
- Inform (SNMPv2) - prześlij informację o zaistniałym zdarzeniu (menedżer do menedżera)
- GetResponse - odpowiedz na żądanie menedżera

Elementy bezpieczeństwa w SNMP

- Uwierzytelnianie (SNMPv2) - procedura umożliwiająca stronie odbierającej sprawdzenie, że komunikat pochodzi z danego źródła i ma właściwy czas. Realizuje się ją przez dołączenie do komunikatu dodatkowej informacji.
- Prywatność (SNMPv2) - ochrona danych przed odczytaniem przez nieupoważnionych odbiorców. Realizuje się ją przez szyfrowanie danych.
- Kontrola dostępu - ograniczenie dostępu menedżera do konkretnego fragmentu MIBa oraz określonego zbioru poleceń.

Społeczności w SNMPv1

Każdy agent w systemie dysponuje swoją własną MIB i ma możliwość kontrolowania dostępu do niej przez wielu menedżerów. Kontrola ta ma następujące aspekty:

- usługa uwierzytelniania - agent może zastrzec prawo dostępu do MIB tylko dla pewnych menedżerów
- ograniczenia dostępu - agent może przydzielać różnych przywilejów różnym menedżerom
- usługa pełnomocnictwa - agent może działać jako pośrednik innych agentów. Wymaga to implementacji poprzednich dwóch usług dla agentów względem których pełniona jest funkcja pośrednika

W celu realizacji wszystkich tych aspektów definiuje się społeczność SNMP.

Społeczności w SNMPv1 cd.

Społeczność to relacje łączące agenta i zbiór menedżerów SNMP w ramach których procedury kontrolne mają określone cechy. Społeczność ma charakter lokalny zdefiniowany u agenta. Agent tworzy społeczność dla żądanej kombinacji cech:

- uwierzytelniania
- kontroli dostępu
- pełnomocnictwa

Każdej społeczności nadaje się unikalną (w ramach agenta) nazwę którą należący do niej agenci muszą podawać przy wszystkich operacjach związanych z danym agentem.

Agent może ustanowić wiele społeczności.

Menedżerowie mogą należeć do wielu społeczności.

Polityka ograniczeń dostępu w SNMPv1

Każdej społeczności SNMP odpowiada profil społeczności określający politykę dostępu do obiektów MIB. Profil taki ma dwa aspekty:

- widok MIB - to zbiór obiektów MIB do których dostęp ma dana społeczność
- tryb dostępu - określa polecenia które możliwe są do wykonania na danym obiekcie. Tryb dostępu w SNMPv1 to następujący zbiór: $\{READ-ONLY, READ-WRITE\}$

Bezpieczeństwo w SNMPv2

środki zapewniania bezpieczeństwa w SNMPv2 służą do ochrony przed następującymi zagrożeniami:

- ujawanianie - przeciwnik może śledzić informacje wymieniane przez menedżera i agenta i w ten sposób poźnać wartość zarządzanych obiektów oraz uzyskać informacje o wydarzeniach
- maskarada - przeciwnik może starać się podszyć pod członka społeczności w celu wykonania niedozwolonej dla siebie operacji
- modyfikacja treści komunikatu - przeciwnik może zmienić wygenerowany przez członka społeczności komunikat w trakcie przesyłania w taki sposób aby doprowadzić do wykonania niedozwolonej operacji zarządzania.

Bezpieczeństwo w SNMPv2 cd.

- modyfikacja kolejności i czasu komunikatów - w celu doprowadzenia do wykonania niedozwolonych operacji przeciwnik może zmieniać kolejność, opóźniać lub powtarzać komunikaty SNMP

SNMPv2 nie chroni natomiast przed następującymi zagrożeniami:

- uniemożliwienie działania - przeciwnik może zablokować wymianę informacji między agentem a menedżerem
- analiza ruchu - przeciwnik może śledzić schemat ruchu pomiędzy menedżerem i agentami

Strony w SNMPv2

Komunikaty SNMPv2 zawierają informacje o tożsamości źródła i miejsca przeznaczenia. Każda jednostka może jednak zachowywać się inaczej pod względem bezpieczeństwa w zależności nie tylko od tożsamości drugiej strony ale także od własnie obsługiwanego programu. Rola jednostki w SNMPv2 zależy więc od kontekstu jej działania. Ideę roli wyraża pojęcie strony. Jednostki mogą obejmować wiele stron.

Każda jednostka SNMPv2 dysponuje bazą danych o zawierającą informacje o wszystkich znanych jej stronach, są to:

- Strony lokalne - zbiór stron na których działania wykonuje lokalna jednostka SNMPv2 czyli zbiór ról tej jednostki
- Strony reprezentowane - zbiór stron jednostek reprezentowanych przez daną jednostkę SNMPv2

- Strony odległe - zbiór stron, których działania realizują inne jednostki SNMPv2 z którymi dana jednostka może wchodzić w interakcje

Formaty komunikatu SNMPv2

privDst	authInfo	dstParty	srcParty	context	PDU

Format ogolny

privDst	LANCUCH OKTETOW dlugosci zero	dstParty	srcParty	context	PDU

Komunikat niezabezpieczony

privDst	wyciag	dstTimestamp	srcTimestamp	dstParty	srcParty	context	PDU

Uwierzytelnianie bez prywatnosci

privDst	LANCUCH OKTETOW dlugosci zero	dstParty	srcParty	context	PDU

Prywatnosc bez uwierzytelniania

privDst	wyciag	dstTimestamp	srcTimestamp	dstParty	srcParty	context	PDU

Prywatnosc i uwierzytelnianie

Prywatność

Dla każdej znanej jednostki SNMPv2 baza danych stron zawiera trzy zmienne których znaczenie zależy od stosowanego protokołu prywatności

- *partyPrivProtocol* - określa protokół prywatności i mechanizm ochrony komunikatów otrzymywanych przez daną strone. Wartość *noPriv* oznacza, że komunikaty otrzymywane przez stronę nie są chronione przez ujawnieniem.
- *partyPrivPrivate* - tajna wartość której wymaga protokół prywatności. Może to być klucz szyfru symetrycznego lub prywatny klucz szyfru asymetrycznego.
- *partyPrivPublic* - dowolna wartość jawna potrzebna w protokole prywatności. Może to być klucz publiczny w systemie asymetrycznym.

Prywatność cd.

Mechanizm zapewniania prywatności w aktualnej wersji SNMPv2 polega na szyfrowaniu z użyciem algorytmu DES i wymaga aby obie strony dzieliły wspólny klucz szyfrujący. Struktura bazy danych umożliwia jednak zastosowanie innych algorytmów szyfrujących (symetrycznych bądź asymetrycznych).

Uwierzytelnianie

Dla każdej strony znanej danej jednostce SNMPv2 baza danych stron zawiera pięć zmiennych, których znacznie jest uzależnione od protokołu uwierzytelniania:

- *partyAuthProtocol* - określa protokół uwierzytelniania stosowany do potwierdzania pochodzenia i nienaruszalności wysyłanych komunikatów. Wartość *noAuth* wskazuje, że komunikaty wysyłane przez stronę nie podlegają uwierzytelnianiu.
- *partyAuthClock* - określa aktualny czas lokalny danej strony
- *partyAuthPrivate* - tajna wartość wymagana przez protokół uwierzytelniania. Może to być tajna wartość hasha z komunikatu, klucz szyfru symetrycznego lub prywatny klucz szyfru asymetrycznego.

Uwierzytelnianie cd.

- *partyAuthPublic* - dowolna wartość jawna potrzebna w protokole uwierzytelniania. Może to być klucz publiczny w systemie asymetrycznym.
- *partyAuthLifetime* - narzucona administracyjnie górna granica akceptowanego opóźnienia dostarczania komunikatów generowanych przez daną stronę

Kontrola dostępu

Na politykę kontroli dostępu składają się cztery elementy:

- strona przeznaczenia - strona SNMP wykonująca operację zarządzania na żądanie strony źródłowej
- strona źródłowa - strona SNMP żądająca wykonania operacji na żądanie stron przeznaczenia
- zasoby - informacje zarządzania, na których można przeprowadzać żądane operacje zarządzania w postaci lokalnego widoku MIB lub relacji pełnomocnictwa, nazywane także kontekstem
- przywileje - operacje dozwolone, zdefiniowane jako dozwolone PDU przynależące do danego kontekstu i do których wykonania w imieniu podmiotu jest uprawniony odbiorca

Kontrola dostępu cd.

Kontrolę dostępu określają informacje zawarte w MIB stron. Baza ta składa się z czterech tablic:

- tablicy stron - zawiera po jednej pozycji na każdą stronę znaną lokalnemu agentowi. Każda pozycja zawiera parametry uwierzytelniania i prywatności. Raz na sekundę lokalny menedżer musi zwiększyć wartość zegara dla każdej pozycji tablicy
- tablica kontekstów - może zawierać pozycje związane z infromacjami lokalnymi oraz relacjami pełnomocnictwa
- tablica kontroli dostępu - jest indeksowana stroną źródłową, stroną przeznaczenia i kontekstem. Każda pozycja zawiera zbiór PDU akceptowanych przez odbiorcę
- tablica widoków MIB - składa się ze zbioru widoków

Architektura jednostki SNMPv3

- Koegzystencja starego i nowego.
- Elementy
  - Jądro SNMP
    - dokładnie jedno dla każdej jednostki,
    - identyfikowane przez snmpEngineID.
  - Aplikacje.

Architektura jednostki SNMP – jądro

```
+-------------------------------------------------------------+
|  jądro SNMP (ident. przez snmpEngineID)                     |
|                                                             |
|  +-------------+ +-------------+ +------------+ +------------+ |
|  |             | |             | |            | |            | |
|  | Rozdzielnik | | Podystem    | | Podsystem  | | Podsystem  | |
|  |             | | Przetwarz.  | | Bezpiecz-  | | Kontroli   | |
|  |             | | Komunikatów | | eństwa     | | Dostępu    | |
|  |             | |             | |            | |            | |
|  +-------------+ +-------------+ +------------+ +------------+ |
|                                                             |
+-------------------------------------------------------------+
```

Architektura jednostki SNMP – aplikacje

```
+-----------------------------------------------------------------+
|  Aplikacje                                                      |
|                                                                 |
|  +--------------+  +---------------+  +---------------+         |
|  | Generator    |  | Odbiornik     |  | Przekaźnik    |         |
|  | Poleceń      |  | Powiadomień   |  | Pośredniczący|          |
|  +--------------+  +---------------+  +---------------+         |
|                                                                 |
|  +--------------+  +---------------+  +---------------+         |
|  | Przetwornik  |  | Nadajnik      |  | Inne          |         |
|  | Poleceń      |  | Powiadomień   |  |               |         |
|  +--------------+  +---------------+  +---------------+         |
|                                                                 |
+-----------------------------------------------------------------+
```

```
+--------------------------------------------------------------------+
| +---------------+  +---------------+  +---------------+  jedn. SNMP  |
| |   NADAJNIK    |  |   ODBIORNIK   |  |   GENERATOR   |              |
| | POWIADOMIEŃ   |  | POWIADOMIEŃ   |  |    POLECEŃ    |              |
| |   aplikacje   |  |   aplikacje   |  |   aplikacje   |              |
| +---------------+  +---------------+  +---------------+              |
|          ^                 ^                  ^                      |
|          |                 |                  |                      |
|          v                 v                  v                      |
|          +--------+--------+------------------+                      |
|                  ^                                                   |
|                  |       +----------------------+  +-----------------+ |
|                  |       | Podsystem przetw.    |  | Podsystem       | |
| Rozdzielnik      v       | Komunikatów          |  | Bezpieczeństwa  | |
| +--------------------+   |     +-------------+  |  |                 | |
| | Rozdzielnik PDU    |   |  +->| v1MP      * |<--->| +-------------+ | |
| |                    |   |  |  +-------------+  |  | | Inny model  | | |
| |                    |   |  |  +-------------+  |  | | Bezpiecz-   | | |
| |                    |   |  +->| v2cMP     * |<--->| | eństwa      | | |
| | Rozdzielnik        |   |  |  +-------------+  |  | +-------------+ | |
| | Komunikatów <---------->+                     |  |                 | |
| |                    |   |  |  +-------------+  |  | +-------------+ | |
| |                    |   |  +->| v3MP      * |<--->| | Model bez-  | | |
| | Odwzorowanie       |   |  |  +-------------+  |  | | pieczeństwa| | |
| | na transport       |   |  |  +-------------+  |  | | op. na uż.  | | |
| | (np. wg RFC1906)   |   |  +->| otherMP   * |<--->| +-------------+ | |
| +--------------------+   |     +-------------+  |  |                 | |
|           ^              +----------------------+  +-----------------+ |
|           |                                                          |
|           v  do sieci                                                |
+--------------------------------------------------------------------+
```

Wysokopoziomowe parametry bezpieczeństwa

- securityModel – zastosowany model bezpieczeństwa:
  - oparty na społecznościach (SNMPv2),
  - oparty na użytkownikach.
- securityName – nazwa osoby, organizacji itp. wykonującej czynności zarządzania,
- securityLevel – wymagany poziom bezpieczeństwa.
  - bez autentyfikacji i poufności (noAuthNoPriv),
  - z autentyfikacją, ale bez poufności (authNoPriv),
  - z autentyfikacją i poufnością (authPriv).

Model bezpieczeństwa

- Opisywany przez liczbę czterobajtową.
- Do 255 standardowych modeli bezpieczeństwa.
- Do 255 modeli bezpieczeństwa dla każdego przedsięwzięcia (identyfikowanego za pomocą bitów starszych od 8.).
- Co daje
  - sprawdza, czy komunikat nie został naruszony,
  - sprawdza autentyczność jednostki, która wygenerowała komunikat,
  - wykrywa, czy komunikat nie jest zbyt przestarzały,
  - odszyfrowuje komunikat, jeśli był zaszyfrowany.
- Możliwość spamiętywania parametrów bezpieczeństwa (jeśli inne niż wynegocjowane).
- Można zarządzać parametrami za pomocą SNMP.

Model kontroli dostępu

- Określa, czy wskazana przez securityName osoba ma dostęp do wykonywania określonej operacji na wskazanym obiekcie.
- Ma operację zapytania, czy dozwolony jest dostęp (isAccessAllowed).
- Można zarządzać parametrami za pomocą SNMP.

Model bezpieczeństwa oparty na użytkowniku (USM) – cele

- Cele standardowe.
- Założenia dodatkowe
  - Obciążenie wygrywa z bezpieczeństwem.
  - Niezależność od zewnętrznych protokołów.
  - Zachowanie dotychczasowej filozofii SNMP.
- Zapewniane usługi
  - integralność danych,
  - uwierzytelnienie pochodzenia danych,
  - poufność danych,
  - ograniczona ochrona przed powtórzeniami.

UMS – podział na moduły

- Moduł uwierzytelnienia
  - integralność danych,
  - uwierzytelnienie pochodzenia danych.
- Moduł czasowy (150 sekund)
  - ochrona przed powtórzeniami,
  - ochrona przed opóźnieniami.
- Moduł ochrony prywatności
  - zapewnienie poufności danych.

UMS – stosowane mechanizmy bezpieczeństwa

- HMAC-MD5-96,
- HMAC-SHA-96,
- CBC-DES,
- czas sprawdzany tylko przy sprawdzaniu integralności danych:
  – autentyfikacja synchronizacji czasu,
  – snmpEngineBoots – liczba uruchomień agenta,
  – snmpEngineTime – czas na maszynie agenta.

UMS – atrybuty użytkownika

- userName – nazwa,
- securityName – nazwa niezależna od modelu bezpieczeństwa,
- authProtocol – czy komunikaty mają być uwierzytelniane i jaki protokół ma być używany,
- authKey – klucz (prywatny) do powyższego uwierzytelniania (różny dla różnych jąder SNMP),
- authKeyChange i authOwnKeyChange – sposób zmiany klucza uwierzytelnienia,
- privProtocol – czy komunikaty mają być szyfrowane i jaki protokół obsługi szyfrowania ma być użyty,
- privKey – klucz (prywatny) do powyższego szyfrowania (różny dla różnych jąder SNMP),
- privKeyChange i privOwnKeyChange – sposób zmiany klucza szyfrowania.

UMS – klucze

- Lokalizacja
  - Hasło jest konwertowane na klucz K_u za pomocą MD5 lub SHA,
  - Z wartości $K_u$snmpEngineIDK_u za pomocą przypisanej użytkownikowi metody generowania hasza generowany jest wyciąg – to jest klucz lokalny.
- Renegocjacja
  - specjalne komunikaty,
  - oparta na tajności starego klucza i losowości.

Model kontroli dostępu oparty na perspektywach (VACM)

- Pamięć lokalnej konfiguracji (Local Configuration Datastore – LCD) zawiera informacje o prawach dostępu.
- Zdefiniowane jest pojęcie grupy (zbiór par securityModel, securityName).
- Prawa są definiowane z uwzględnieniem securityLevel.
- Dla każdego kontekstu (adresu w MIB) może być ustalona perspektywa: określa się typy (i opcjonalnie instancje typów), do których jest dostęp.
- Perspektywy są definiowane przez
  - poddrzewa perspektywy,
  - rodziny drzew perspektywy (maski bitowe).

- Każda grupa ma perspektywy
  - odczytu,
  - zapisu,
  - powiadamiania.