RMON II

RMON2 - Úvod

- prostředek pro centralizované sledování velkého množství podsítí
- offline operace - samostatná práce sondy bez nutnosti kontinuálního sledování monitorovací stanicí
  - nižší komunikační zátěž
  - odolnost proti chybám
- proactive monitoring - nepřetržitý běh diagnostiky
  - autonomní záznam statistik i historie
  - umožňuje dodatečnou analýzu chyb
- problem detection and reporting
  - schopnost sondy rozpoznat některé události
  - možnost volby zpracování (trap, zpracování sondou)
- value added data - provádění analýzy dat zachycených na segmentu
- multiple managers - souběžná obsluha více řídicích stanic

RMON2 - Základní pojmy

- **Terminologie**
  - protokol základní úrovně
  - protokol síťové úrovně
  - protokoly aplikační úrovně
- **Obecná struktura tabulek**
  - řídicí tabulky - informace o datech v datových tabulkách
  - datové tabulky - ukládání naměřených hodnot
- **Práce s tabulkami**
  - tabulky se mohou indexovat více sloupci
  - index v tabulce může mít proměnnou délku - OID - Object Identifier
  - index může tvořit i sloupec cizí tabulky
  - jeden sloupec se může objevit vícekrát vrůzných

RMON2 - Základní pojmy

- Řídicí tabulky
  - identifikují zdroj (rozhraní) ze kterého se získávají data
  - DataSource - ifIndex v tabulce interfaces
  - DroppedFrames - úspěšně přijaty, ale nezahrnuty do statistik
  - Owner - vlastník řádky (vícenásobný přístup)
  - Status - stav řádky
    - » active - používána (R/W)
    - » notInService - existuje, není používána (R/W)
    - » notReady - existuje, ale chybí informace (R/W)
    - » createAndGo - vytvořit a přechod na active (W)
    - » createAndWait - vytvořit (W)
    - » destroy - smazat spolu se souvisejícími řádky v podřízených tabulkách (W)

RMON2 - Základní pojmy

- Datové tabulky
  - vztahy určeny pomocí indexu
  - součástí indexu je i index jedné nebo více řídicích tabulek
  - přidávání položek do datové tabulky z nadřízené entity
    - » Inserts
    - » Deletes
    - » MaxDesiredEntries (-1) - neomezeně
  - časově filtrované hodnoty - řádky, které se změnily od jisté doby
    - » TimeMark - obshuje sysUpTime (get-bulk)
    - » změna nejpozději 5s od změny ostatních dat
  - položka CreateTime - čas vytvoření položky

Skupiny RMON 2

Skupiny:

- Adresář protokolů
- Distribuce protokolů
- Mapa adres
- Host systémy síťové úrovně
- Matice hostů síťové úrovně
- Host systémy aplikační úrovně
- Matice hostů aplikační úrovně
- Historie
- Konfigurace sondy

RMON2 - Adresář protokolů (Protocol Directory)

- protocolDirTable - nejdůležitější tabulka
- omezená rozšiřitelnost
  - každá sonda umí pracovat s omezenou množinou protokolů, neumí se naučit protokoly za běhu
  - dekódování paketu provádí programové vybavení podle tabulky
  - např. sonda "umí" IP a UDP, rozpozná DNS a SNMP, omezená rozšiřitelnost - přidání TFTP a NTP
- protocolDirLastChange - časová značka (sysUpTime)
- protcolDirTable - vlastní tabulka
  - tabulka se rozšiřuje pomocí příkazu set s daným protocolDirID
  - nezná-li sonda ID protokolu, pak jej odmítne

RMON2 - Adresář protokolů (Protocol Directory)

- Tabulka obsahuje
  - protocolDirID
  - protocolDirParameters
  - protocolDirLocalIndex
  - protocolDirDescr
  - protocolDirType
  - protocolDirAddressMapConfig
  - protocolDirHostConfig
  - protocolDirMatrixConfig
  - protocolDirOwner
  - protocolDirStatus

RMON2 - Adresář protokolů (Protocol Directory)

- Indexování ProtocolDirTable
  - agregovaný index složený z
    - » protocolDirID ether2.ip.tcp.http
    - » protocolDirParameters
- index
  - linková vrstva - délka (4) nebo (8)
    - » ether2 - 0.0.0.1
  - síťová vrstva - délka (4)
    - » dle typu protokolu (assigned numbers)
  - aplikační vrstva - délka (4)
    - » dle hodnoty portu (assigned numbers)
- agregovaný index pro HTTP

16. 0.0.0.1. 0.0.8.0. 0.0.0.6. 0.0.0.80. 4. 0.0.0.0

RMON2 - Distribuce protokolů (Protocol Distribution)

- shromažďování informace o paketech a oktetech různých protokolů detekovaných na segmentu sítě
- obsahuje dvě tabulky
  - protocolDistControlTable
  - protocolDistStatsTable
- **protocolDistControlTable**
  - řídicí tabulka
  - tabulka obsahuje
    - » Index
    - » DataSource
    - » DroppedFrames
    - » CreateTime
    - » Owner
    - » Status
- **protocolDistStatsTable**
  - datová tabulka
  - tabulka obsahuje
    - » Pkts
    - » Octets

RMON2 - Mapa adres (Address Map)

- mapování síťových adres na adresy linkové úrovně
- obsahuje dvě tabulky
  - addressMapControlTable
  - addressMapTable
- proměnné
  - addressMapInserts - celkový počet přidaných položek
  - addressMapDeletes - celkový počet smazaných položek
  - addressMapMaxDesireEntries - maximální velikost tabulky
- **addressMapControlTable**
  - řídicí tabulka
  - tabulka obsahuje
    - » Index, DataSource, DroppedFrames, Owner, Status
- **addressMapTable**
  - datová tabulka
  - tabulka obsahuje
    - » TimeMark, NetworkAddress, Source, PhysicalAddress, LastChange

RMON2 - Mapa adres (Address Map)

- indexování
  - addressMapTimeMark - čas
  - protocolDirLocalIndex - protokol síťové úrovně
  - addressMapNetworkAddress - síťová adresa
  - addressMapSource - linková adresa

RMON2 - Host systémy síťové úrovně (Network Layer Host)

- zachycuje počty paketů a oktetů daného protokolu síťové úrovně přijatých nebo vyslaných z jednotlivých síťových adres na specifikovaném rozhraní
- obsahuje dvě tabulky
  - hlHostControlTable
  - nlHostTable

- hlHostControlTable
  - řídicí tabulka
  - tabulka obsahuje
  - » Index, DataSource, NlDroppedFrames, NlInserts, NlDeletes, NlMaxDesiredEntries,AlDroppedFrames, AlInserts, AlDeletes, AlMaxDesiredEntries,Owner , Status

- nlTableTable
  - datová tabulka
  - tabulka obsahuje
  - » TimeMark, Address, InPkts, OutPkts, InOctets, OutOctets, OutMacNonUnicastPkts, CreateTime

RMON2 - Matice hostů síťové úrovně (Network Layer Host)

- indexování v řídicí tabulce hlHostControlTable
  - hlHostControlIndex
- indexování v datové tabulce nlHostTable
  - hlHostControlIndex - index řídicí tabulky
  - nlHostTimeMark - časový filtr
  - protocolDirLocalIndex - identifikace protokolu síťové úrovně
  - nlHostAddress - síťová adresa

RMON2 - Matice hostů síťové úrovně (Network Layer Matrix)

- čítá počty paketů a oktetů mezi dvěma síťovými adresami. Rozlišuje spojení tam a zpět. Vybírá N nejaktivnějších spojení.
- zahrnuje pět tabulek
  - nlMatrixControlTable - řídicí tabulka
  - nlMatrixSDTable - tabulka pro jeden směr
  - nlMatrixDSTable - tabulka pro druhý směr
  - nlMatrixTopNControlTable - řídicí tabulka pro prvních N
  - nlMatrixTopNTable - tabulka pro prvních N

RMON2 - Matice hostů síťové úrovně (Network Layer Matrix)

- **hlMatrixControlTable - řídicí tabulka pro síťovou i aplikační vrstvu**
  - **tabulka obsahuje**
    - » **Index - jednoznačný index tabulky**
    - » **DataSource - sledovaný interface**
    - » **NlDroppedFrames - ztracené (nezapočítané) rámce**
    - » **NlInserts - čítač přidání položky do matice**
    - » **NlDeletes - čítač rušení položky v matici**
    - » **NlMaxDesiredEntries - maximální očekávaný počet položek**
    - » **AlDroppedFrames - ztracené (nezapočítané) rámce**
    - » **AlInserts - čítač přidání položky do matice**
    - » **AlDeletes - čítač rušení položky v matici**
    - » **AlMaxDesiredEntries - maximální očekávaný počet položek**
    - » **Owner - vlastník položky**
    - » **Status - stav položky**

16

RMON2 - Matice hostů síťové úrovně (Network Layer Matrix)

- **nlMatrixSDTable, nlMatrixDSTable**
  - **datová tabulka**
  - **tabulka obsahuje**
  - **TimeMark - časový filtr**
  - **SourceAddress - síťová adresa**
  - **DestAddress - síťová adresa**
  - **Pkts - čítač paketů**
  - **Octets - čítač oktetů**
  - **CreateTime - čas vytvoření**
- **nlMatrixTopNTable**
  - **datová tabulka**
  - **tabulka obsahuje**
  - **Index - jednoznačný index**
  - **ProtocolDirLocalIndex - index síťového protokolu**
  - **SourceAddress - síťová adresa**
  - **DestAddress - síťová adresa**
  - **PktRate - čítač paketů**
  - **ReversePktRate - čítač paketů v opačném směru**
  - **OctetRate - čítač oktetů**
  - **ReverseOctetRate - čítač oktetů v opačném směru**

17

RMON2 - Matice hostů síťové úrovně (Network Layer Matrix)

- **nlMatrixTopNControlControlTable**
  - **řídicí tabulka pro síťovou vrstvu**
  - **tabulka obsahuje**
    - » **Index - jednoznačný index tabulky**
    - » **MatrixIndex - index do TopN tabulky**
    - » **RateBase - počet oktetů a paketů**
    - » **TimeRemaining - zbývající čas pro shromažďování dat**
    - » **GenerateReports - čítač generovaných zpráv**
    - » **Duration - počet sekund shromažďování dat**
    - » **RequestedSize - maximální počet požadovaný počet položek v reportu**
    - » **GrantedSize - počet položek matice v reportu**
    - » **StartTime - poslední start reportu (sysUpTime)**
    - » **Owner - vlastník položky**
    - » **Status - stav položky**

18

RMON2 - Matice hostů síťové úrovně (Network Layer Matrix)

- indexování v řídicí tabulce hlMatrixControlTable
  - hlMatrixControlIndex
- indexování v datové tabulce nlMatrixSDTable
  - hlMatrixControlIndex - index řídicí tabulky
  - nlMatrixSDTimeMark - časová značka
  - protocolDirLocalIndex - určení protokolu síťové úrovně
  - nlMatrixSDSourceAddress - síťová adresa zdrojového uzlu
  - nlMatrixSDDestAddress - síťová adresa cílového uzlu
- indexování v datové tabulce nlMatrixDSTable
  - hlMatrixControlIndex - index řídicí tabulky
  - nlMatrixDSTimeMark - časová značka
  - protocolDirLocalIndex - určení protokolu síťové úrovně
  - nlMatrixDSSourceAddress - síťová adresa zdrojového uzlu
  - nlMatrixDSDestAddress - síťová adresa cílového uzlu

RMON2 - Matice hostů síťové úrovně (Network Layer Matrix)

- indexování v řídicí tabulce hlMatrixTopNControlTable
  - hlMatrixTopNControlIndex
- indexování v datové tabulce nlMatrixTopNTable
  - hlMatrixTopNControlIndex - index řídicí tabulky
  - nlMatrixTopNIndex - index datové tabulky

RMON2 - Host systémy aplikační úrovně (Application Layer Host)

- zachycuje počty paketů a oktetů daného protokolu aplikační úrovně přijatých nebo vyslaných z jednotlivých síťových adres na daném rozhraní
- obsahuje dvě tabulky
  - hlHostControlTable
  - alHostTable
- hlHostControlTable
  - řídicí tabulka
  - tabulka obsahuje
    - » Index, DataSource, NlDroppedFrames, NlInserts, NlDeletes, NlMaxDesiredEntries,AlDroppedFrames, AlInserts, AlDeletes, AlMaxDesiredEntries,Owner , Status
- nlTableTable
  - datová tabulka
  - tabulka obsahuje
    - » TimeMark, InPkts, OutPkts, InOctets, OutOctets, CreateTime

RMON2 - Host systémy aplikační úrovně (Application Layer Hosts)

- indexování v řídicí tabulce
  - hlHostControlIndex
- indexování v datové tabulce
  - hlHostControlIndex - index řídicí tabulky
  - alHostTimeMark - časová značka
  - protocolDirLocalIndex - určení protokolu síťové úrovně
  - nlHostAddress - síťová adresa
  - protocolDirLocalIndex - určení čítaného protokolu

RMON2 - Matice hostů aplikační úrovně (Application Layer Matrix)

- čítá počty paketů a oktetů mezi dvěma síťovými adresami předávanými mezi dvěma aplikacemi. Rozlišuje spojení tam a zpět. Vybírá N nejaktivnějších spojení.
- zahrnuje pět tabulek
  - nlMatrixControlTable - řídicí tabulka společná se skupinou Network Layer Matrix
  - alMatrixSDTable - tabulka pro jeden směr
  - alMatrixDSTable - tabulka pro opačný směr
  - alMatrixTopNControlTable - řídicí tabulka pro prvních N
  - alMatrixTopNTable - tabulka pro prvních N

RMON2 - Matice hostů aplikační úrovně (Application Layer Matrix)

- alMatrixSDTable, alMatrixDSTable a alMatrixTopNTable
  - datová tabulka
  - tabulka obsahuje
  - TimeMar - časový filtr
  - Pkts - čítač paketů
  - Octets - čítač oktetů
  - CreateTime - čas vytvoření položky (sysUpTime)
  - datová tabulka
  - tabulka obsahuje
  - Index - jednoznačný index
  - ProtocolDirLocalIndex - index síťového protokolu
  - SourceAddress - síťová adresa
  - DestAddress - síťová adresa
  - ProtocolDirLocalIndex - typ protokolu
  - PktRate - čítač paketů
  - ReversePktRate - čítač paketů v opačném směru
  - OctetRate - čítač oktetů
  - ReverseOctetRate - čítač oktetů v opačném směru

RMON2 - Matice hostů aplikační úrovně (Application Layer Matrix)

- alMatrixTopNControlControlTable
  - řídicí tabulka pro aplikační vrstvu
  - tabulka obsahuje
    - » Index - jednoznačný index tabulky
    - » MatrixIndex - index do TopN tabulky
    - » RateBase - počet oktetů a paketů
    - » TimeRemaining - zbývající čas pro shromažďování dat
    - » GeneratedReports - čítač generovaných zpráv
    - » Duration - počet sekund shromažďování dat
    - » RequestedSize - maximální počet požadovaných položek matice reportu
    - » GrantedSize - počet položek v reportu
    - » StartTime - poslední start reportu (sysUpTime)
    - » Owner - vlastník položky
    - » Status - stav položky

RMON2 - Matice hostů aplikační úrovně (Application Layer Matrix)

- indexování v řídicí tabulce hlMatrixControlTable
  - hlMatrixControlIndex
- indexování v datové tabulce alMatrixSDTable
  - hlMatrixControlIndex - index řídicí tabulky
  - alMatrixSDTimeMark - časová značka
  - protocolDirLocalIndex - určení protokolu síťové úrovně
  - nlMatrixSDSourceAddress - síťová adresa zdrojového uzlu
  - nlMatrixSDDestAddress - síťová adresa cílového uzlu
  - protocolDirLocalIndex - určení čítaného protokolu
- indexování v datové tabulce nlMatrixDSTable
  - je totožné s výše uvedenou tabulkou (pouze místo SD -> DS)

RMON2 - Matice hostů aplikační úrovně (Application Layer Matrix)

- indexování v řídicí tabulce alMatrixTopNControlTable
  - alMatrixTopNControlIndex
- indexování v datové tabulce nlMatrixTopNTable
  - alMatrixTopNControlIndex - index řídicí tabulky
  - alMatrixTopNIndex - index datové tabulky

RMON2 - Skupina historie (User History)

- dovoluje zachycovat data podle přání uživatele. Nahrazuje typickou funkci řídících stanic - periodické dotazování.
- k označení se používá MIB instance
- data mohou být typu INTEGER
- obsahuje tři tabulky
  - usrHistoryControlTable - řídicí tabulka
  - usrHistoryObjectTable - tabulka identifikátorů objektů
  - usrHistoryTable - tabulka hodnot objektů

RMON2 - Skupina historie (User History)

- Řídicí tabulka
  - Index - jednoznačný index položky
  - Objects - počet shromažďovaných objektů
  - BucketsRequested - počet požadovaných časových intervalů
  - BucketsGranted - aktuální počet
  - Interval - délka intervalu v sekundách
  - Owner - vlastník
  - Status - stav
- Datová tabulka usrHistoryObjectTable
  - Index - jednoznačný index položky
  - Variable - identifikátor objektu
  - SampleType - typ ukládání - absolutní/rozdílové

RMON2 - Skupina historie (User History)

- Datová tabulka usrHistoryEntry
  - SampleIndex - jednoznačný index položky
  - IntervalStartVariable - začátek intervalu vzorkování
  - IntervalEnd - typ ukládání - konec intervalu vzorkování
  - AbsValue - absolutní hodnota vzorkování
  - ValStatus - určuje znaménko hodnoty a dostupnost

RMON2 - Skupina historie (User History)

- indexování v řídicí tabulce
  - usrHistoryControlIndex
- indexování v datové tabulce usrHistoryObjectTable
  - usrHistoryControlIndex - index řídicí tabulky
  - usrHistoryObjectIndex - index objektu
- indexování v datové tabulce usrHistoryObjectTable
  - usrHistoryControlIndex - index řídicí tabulk
  - usrHistorySampleIndex - index vzorku
  - usrHistoryObjectIndex - index objektu

RMON2 - Skupina konfigurace sondy (Probe Configuration)

- řídí konfiguraci různých parametrů sondy
- dovoluje určit které skupiny sonda zpracovává
- dovoluje zavádět programové vybavení z TFTP serveru
- dovoluje provádět reset sondy
- dovoluje komunikovat se sondou pomocí seriového rozhraní (modem, komutované spoje)
- dovoluje nastavit parametry síťového rozhraní
  - IP adresu, masku sítě, adresu směrovače
- dovoluje nastavit tabulku adres hostů pro zpracování asynchronních událostí (trap)

Prostředky pro řízení počítačových sítí

Akademie informačních technologií
6. dubna 1998
Plzeň

Řídicí stanice - SNMP monitory

- periodické dotazování na stav agentů
- příjem a zpracování asynchronních událostí
  - » automatická reakce na došlé alarmy
- kompletní vyhodnocení a prezentace
  - » grafické uživatelské rozhraní
  - » mapy sítě, jejich automatické vytvoření
  - » seskupování zařízení do logckých celků
  - » grafická prezentace získaných dat
- doplňkové služby
  - » telnet
  - » ping
  - » Trascend

Příklady monitorů

- **Platformy**
  - UNIX
  - DOS (Windows)
- **Příklady**
  - SunNet Manager (SUN, Solaris)
  - OpenView NNM (HP-UX, SUN)
  - NetView (IBM, AIX)
  - D-View (D-Link, MS-Windows)

Zhodnocení

- jednoduchá autentifikace
- zatěžování sítě při čtení rozsáhlých tabulek
- zatěžování sítě při periodickém monitorování
- postrádá přímou podporu pro distribuované řízení
- není kompatibilní s novější verzí SNMPv2
- zavedení RMON (Remote Monitoring)