Inhaltsverzeichnis

Monitore

Ein Monitor ist ein Hilfsmittel, mit dem man Aktivitäten eines Systems überwachen kann.
Im Allgemeinen überwachen Monitore die Systemperformance, sammeln statistische Informationen, analysieren Daten, und stellen die Ergebnisse dar.
Einige identifizieren ebenfalls Problembereiche und beheben eventuelle Schäden.

Ein Systemadministrator nutzt ein solches Programm für Verkehrsmessungen, um die Performance der Netzsegmente zu steigern.
Die Netzwerkanalyser erfassen hierzu die Eck- oder Grunddaten des Netzes, also beispielsweise:
– die Netzlast,
– welche Stationen mit welchen anderen (Pair Statistic) kommunizieren,
– die Fehlerrate (physikalische Fehler im Ethernet und MAC-Fehlermeldungen im Token-Ring-Protokoll),
– den Anteil der verschiedenen Protokolle,
– die Server-Auslastung,
– die Latenzzeiten zwischen Server und Clients sowie
– die Auslastung von Routern.
Die Ergebnisse der Netzwerkstatistik sind somit eine entscheidende Voraussetzung,
um im Fehlerfall die Störung physikalisch und logisch einzugrenzen. Nur mit konstant betriebener Netzwerkstatistik kann der Administrator das Verhalten des eigenen Netzwerks bestimmen und Veränderungen visualisieren, um rechtzeitig bei kritischen Entwicklungen Maßnahmen zur Abhilfe einleiten zu können.

Fachbegriffe aus dem Bereich

Im Folgenden werden einige Begriffe aus dem Bereich beschrieben:

- **Event**: Verändern eines Zustandes im System, wie zum Beispiel das Suchen auf einem Datenträger.
- **Trace**: Ein Trace ist die Mitschrift von Ereignissen über einen Zeitraum.
- **Overhead:** Der Overhead beschreibt die Nutzung von Speicher und CPU Leistung. Dieser Overhead senkt die zur Verfügung stehende Systemleistung für andere Aufgaben. Ziel ist es beim Entwurf eines solchen Monitors diesen Overhead zu minimieren.
- **Domain:** Die Domain beschreibt den Umfang der möglichen Aktionen des Monitors.
- **Input Rate:** Ist die maximale Frequenz von Ereignissen, die ein Monitor korrekt beobachten kann. Man unterscheidet zwischen zwei Modi:
  burst - Mode für kurze Zeiträume und sustained - Mode für größere Zeiträume.
- **Resolution:** Beschreibt die Genauigkeit des Darstellungsbereiches.
- **Input Width:** Anzahl der Bits der Abtastung.

Monitorklassifizierung

Monitorprogramme werden eingeteilt nach verschiedenen Charakteristiken wie ihren Implementierungsgrad, Trigger Mechanismus und die Darstellung der Ergebnisse.

Implementierungsgrad (-level):

- Softwaremonitor, Hardwaremonitor, Firmwaremonitor oder Hybridmonitor.
  (Ein Hybridmonitor ist eine Mischung aus den drei zuerst genannten Arten.)

Triggermechanismus:

- Ereignisorientiert (Event-driven): Auslösen einer Aufzeichnung resultierend aus einem Ereignis- oder Zustandswechsel.
- Samplingmonitor. Zeitgesteuerte Auslösung durch Interrupts.

Darstellung der Ergebnisse:

- Online monitors: Kontinuierliche Darstellung oder die Darstellung des Systemzustandes in Intervallen.
- Batch monitors: Datenerfassung mit späterer Auswertung durch ein getrenntes Programm.

Software Monitors

Sie werden eingesetzt zur Überwachung von Netzwerken und Datenbanken. Dabei muss das Programm zur korrekten Abtastung der Daten Mindestanforderungen an die Prozessorgeschwindigkeit und den Speicherbedarf stellen

Im Allgemeinen haben Softwaremonitore geringere Eingangsraten und erfordern eine höhere Systemleistung. Jedoch verfügen sie über eine höhere Aufzeichnungskapazität als die Hardwarelösungen, und sie sind einfacher zu entwickeln und zu modifizieren.

Software Monitor Design

Auf welche Merkmale ist zu achten:

1. Aktivierungsmechanismus:
   - ? **Trap Instruction:** Auslösen eines Software interrupts durch einen Trap
   - ? **Trace Mode:** Der Prozessor wird nach der Ausführung jedes Befehls unterbrochen und eine UP Routine erfasst die Daten.Diese Methode erzeugt einen hohen Overhead.
   - ? **Timer interrupt:** Sampling Funktion über eine Intervallsteuerung
2. **Buffer Size:** Ein großer Arbeitsspeicher minimiert den Zeitaufwand für eine Datensicherung auf einem nichtflüchtigen Speichermedium. Ist er jedoch zu groß, geht zuviel Zeit durch das Erstellen der Kopie verloren.
3. **Number of Buffers:** Minimal zwei Arbeitsspeicher Bereiche, damit Datenerfassung und Datensicherung simultan ablaufen können. Anordnung der Speicher in einem Ringsystem.
4. **Buffer Overflow:** Datensicherung bevor es zu einer Überlaufsituation kommt.
5. **Data Compression or Analysis:** Die erfassten Daten können gleichzeitig betrachtet und verarbeitet werden. Jedoch steigert dieser Zusammenhang den Overhead.
6. **ON/OFF Switch:** Einschalten der Aufzeichnung aus Bedingungen (Filter!).
7. **Language:** z.B.: C;
8. **Priority:** Prioritätssteuerung durch die Software möglich
9. **Abnormal-Events Monitoring:** Neben den bekannten Protokollabläufen auch andere Situationen wie Systeminitialisierungen aufzeichenbar.

Hardware Monitors

Eine Hardwarelösung stellt im Allgemeinen höhere Eingangsraten zur Verfügung.

Ein Hardware Monitor besteht aus folgenden Komponenten: Probes, Counters, Logic Elements, Comparators, Mapping Hardware, Timer und Speicherelement.

Gegenüberstellung der Monitorarten

Diese Aufstellung enthält nur die wichtigsten Kriterien:

Kriterium	***Hardware***	***Software***
Eingangsrate	Groß	Klein
Zeitauswertung	Bereich ns	Bereich ms
Speicherkapazität	Begrenzt durch eingesetzte Speicher.	Begrenzt durch verursachten Overhead.
Overhead	Keinen	Abhängig von der Eingangsrate
Fehler	Falscher Anschluss	Selten
Kosten	Hoch	Mittel

Beide Monitorarten können Fehler beinhalten, die zu Fehlern in den Vergleichsdaten führen können.

Durch die ausgereifte und gründlich programmierte Software sind Fehler eher selten. Bei den Hardwaremonitoren werden Fehler durch falsche Einstellungen erzeugt.

Abschließend ist noch zu erwähnen, dass die Hardwarelösung die teurere Variante ist.

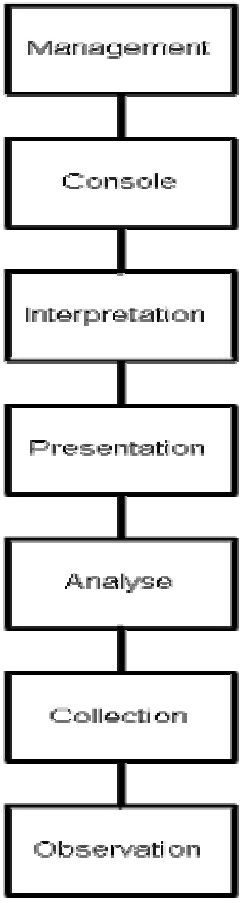
Firmware und Hybrid Monitore

Firmware Monitore werden durch die Veränderung der Programmierung des Mikroprozessors implementiert. Dies ist nützlich wenn Anwendungen an die Grenze zwischen Hardware und Software monitoring fallen. In den meisten Punkten ähneln sich Software und Hardware Monitore.
Firmware Monitore werden dort eingesetzt wo die bestehenden Schnittstellen einfach programmiert werden können. Ein Monitor der aus einer Kombination aus Software, Hardware oder Firmware besteht wird als Hybrid Monitor bezeichnet. Ein Hybrid Monitor verbindet jeweils die Vorteile von Software und Hardware Monitoren. Der Hardware Monitor ist auf dem Board fest installiert und überwacht den Verkehr auf dem Systembus. Der Softwareteil kann die Benutzer Kennung, Prozessor Einstellungen und System Identifikation auslesen.

Distributed – System Monitors

Da die meisten Computer Systeme aus vielen Hardware und Software Komponenten bestehen, die zusammenarbeiten, ist das Monitoring schwierig. Bei zentralisierten Systemen kann an einer zentralen Stelle Monitoring betrieben werden. Bei den verteilten Systemen muss der Monitor an vielen Stellen die Messungen vornehmen. Der Monitor besteht aus mehreren Komponenten die verteilt auf dem System unabhängig voneinander Arbeiten. Um den Umfang der Funktionen des verteilten Monitors besser zu veranschaulichen werden die Funktionen in einer Layer Form dargestellt.

Layer Sicht eines verteilten System Monitors



1.Observation:

Dieser Layer sammelt Rohdaten von individuellen Komponenten des Systems. Im allgemeinen hat jede Komponente ihren eigenen Observer. Deshalb gibt es mehrere Observer auf den unterschiedlichen Subsystemen.

2.Collection

Hier werden die Daten von den verschiedenen Observern gesammelt. Es ist wichtig bei großen Systemen mehrere Kollektoren zu haben, um die einzelnen Netzteil Monitoren zu können.

3.Analysis

Auf diesem Layer laufen Statistic-Routinen die, die Datencharakteristik sammeln.

4.Presentation

Diese Komponente des Monitors erstellt Berichte und gibt bei bestimmten Ereignissen Alarm.

5.Interpretation

Diese Schicht stellt die Schnittstelle zum Menschen her und kann die Daten interpretieren und Aussagen über den Inhalt treffen. Es werden hierfür Regeln benötigt, mit denen die Auswertung realisiert wird.

6.Console

Diese Komponente sieht ein Interface vor, über das die System-Parameter und der Status kontrolliert wird. Diese Monitoring und Kontrollfunktionen werden häufig zusammen genutzt.

7.Management

Die Entscheidung, Änderungen vorzunehmen, wird aufgrund der Parameter getroffen.

Ein Monitor kann aus mehreren Komponenten jeder Schicht bestehen. Es ist z.B. denkbar, dass ein einziger Observer die Daten zu mehreren Collectoren sendet. Die meisten verteilten Systeme sind Mischformen. Sie verwenden Software-, Hardware-, Firmwaremonitore und werden vom Menschen administriert.

Observation (Beobachtung)

Die unterste Schicht des Monitors wird als Beobachtungsschicht bezeichnet und sammelt die Rohdaten. Es gibt drei verschiedene Beobachtungsmechanismen.

Implicit spying

(uneingeschränkte Beobachtung)
Dieser beobachtet wahllos die Aktivität auf dem System Bus oder der Netzwerkverbindung.
Diese Technik wird häufig verwendet, um Local Area Networks zu beobachten, da jede Station jede Unterhaltung mitbekommt und wahlweise eine Station beobachtet werden kann.
Der Vorteil der Technik ist, dass die Performance des Systems nicht beeinträchtigt wird.
Man hat die Möglichkeit zusätzlich Filter zu definieren um nicht relevante Informationen zu vernachlässigen. Nicht jede Information ist dem Benutzer von Bedeutung. Filter helfen einem bei der Entscheidung.
Generell bestehen Filter aus Auswahlkriterien folgender Art:
“boolean”, “arithmetic” oder ”set membership“.

Explicit instrumenting

(eingeschränkte Beobachtung)
Spezielles Beobachten verbindet verschiedene Messpunkte im System untereinander. Dieses Verfahren verursacht zusätzlichen Overhead im System. Jede Komponente im System, die beobachtet wird, muss einzeln administriert werden.

Probing

Beim Probing werden Anfragen an das System gestellt, um die Performance festzustellen. Es werden z.B. speziell markierte Pakete zu einem Ziel geschickt. Das Ziel schickt diese zurück.
Man erhält Informationen über den Durchsatz des Netzes und den Datenverkehr auf der Leitung.

Collection (Sammlung)

Der Teil des Monitors, der die Daten sammelt, wird als Collector bezeichnet. In einem Computernetzwerk hat jeder Computer seinen eigenen Beobachter. Der Collector sammelt die Daten aller Beobachter. Diese Art des Beobachtens erzeugt einen noch größeren Overhead.
Die Beobachter können auf einem oder mehreren Layern arbeiten. Die Netzwerk-Collectoren erhalten ihre Daten von Teilnetz-Collectoren, diese wiederum von Observern jeder Station.
Beim Datensammeln ist es wichtig eine zeitliche Synchronisation zu erreichen, damit die Datenpakete aus den einzelnen Teilnetzen in der richtigen Reihenfolge wieder zusammengesetzt werden können.

Analysis

Die Arbeit von Analyzern ist im Vergleich zu der einfachen Arbeit der Observer sehr kompliziert.
Das Kriterium, welches die Funktion bestimmt, die in dem Analyse Layer platziert werden, ändert sich häufig. Die Ereignisse und die Menge der zu analysierenden Daten während einer Analyse bestimmen, ob die Funktion in dem Observer oder in den Analyzer platziert wird. Um z.B. feststellen zu können, welche Verbindung die höchste Fehlerrate hat, müssen alle Verbindungen im Netzwerk untersucht werden. Es wäre unsinnig nur eine Station zu untersuchen. Diese Funktion kann nicht im Observer ausgeführt werden. Sie muss im Analyzer platziert werden.
Wenn die Analyse Funktion zu zeitintensiv ist, wäre es ratsam, die Daten mitzuschneiden (record) und später zu Analysieren.
Es ist wichtig die Funktion in dem Observer so weit wie möglich zu vereinfachen, um die Belastung dieser zu reduzieren.

Presentation

Der Presentation Layer arbeitet mit der Schnittstelle Mensch zusammen. Er ist so vorbereitet, dass der Benutzer seine Anfragen an den Monitor stellen kann. Er veranschaulicht dem Benutzer die Ergebnisse des Monitors. Diese Schicht ist an die Applikation, mit der der Monitor benutzt wird, gebunden.

Der Monitor sollte in der Lage sein, eine Zusammenfassung über einen bestimmten Zeitpunkt in der Vergangenheit zu geben. Außerdem eine Stunden-, Tages-, Wochen- und Monatszusammenfassung zu erstellen. Hierbei ist es wichtig, dass die Zusammenfassungen aufeinander aufbauen. Die Tageszusammenfassung wird aus den Stundenzusammenfassungen generiert.

Die Bereitstellung der Daten sollte möglichst strukturiert sein, es muss möglich sein, aus jedem Element im Netz eine Zusammenfassung zu erhalten. Das kann ein Router, ein Netzsegment oder ein Host sein.

Der Presentation Layer bietet noch folgende Eigenschaften:

- Alarm Mode: stellt dem Administrator einen Service zur Verfügung, mit dem er sich bei bestimmten Ereignissen benachrichtigen lassen kann.
- Ansprechen des Interface über Menüs. Wenige Bedienungskenntnisse sind erforderlich
- Hintergrundaktivität, Background-Mode

Es gibt drei wichtige Arten des Monitoring :

1. Performance Monitoring

   Beim Performance Monitoring wird im Allgemeinen der Durchsatz, die Antwortzeit und der Ressourcenverbrauch dargestellt. Es können Statistiken über die o.g Ereignisse erstellt werden und diese dann auch strukturiert ausgegeben werden.

2. Error Monitoring

   Beim Error Monitoring werden die Fehler im System beobachtet. Es ist nicht wichtig, was die einzelnen Benutzer machen, sondern wo die Fehler auftreten.

3. Configuration Monitoring

   Beim Configuration Monitoring wird der Durchsatz des Systems gemessen, der User kann aber auswählen, welche Teile des Systems er beobachten möchte.

   Es können somit z.B. unbekannte Stationen festgestellt werden, die sich im Netzwerk befinden.

Interpretation

Um Daten interpretieren zu können, werden Regeln benötigt die genau beschreiben, welche Information ausgewertet werden sollen. Um eine automatische Warnung an den System Administrator zu senden, müssen diese Regeln so konfiguriert werden, das bei bestimmten Ereignissen eine Meldung erzeugt wird!

Console Functions

Mit diesen Funktionen ist es dem System Administrator möglich, die Systemparameter zu verändern, eine neue Konfiguration vorzunehmen und einzelne Komponenten ein- oder auszuschalten.
Leider werden die Consolen und die Monitore häufig von verschiedenen Herstellern geliefert und laufen nicht zusammen auf einer Workstation.