

## indev:s ServerMonitoring (iSM) (Stand Januar 2008)



### Ausgangssituation:

Die IT Infrastruktur ist für die meisten Unternehmen eine der wichtigsten Ressourcen für die täglichen Geschäftsprozesse. Ein Ausfall oder eine Störung der Server-, LAN- und WAN-Verbindungen hat zumeist unmittelbare finanzielle Folgen für das betroffene Unternehmen.

Backup-Systeme und Redundanzen sollen die Verfügbarkeit der installierten Systeme sicherstellen und im Fehlerfall den Betrieb übernehmen.

Derzeit bieten nahezu alle Systeme die Möglichkeit einer Überwachung des laufenden Betriebs. Diese Überwachung, auch Monitoring genannt, liefert den verantwortlichen Administratoren zuverlässig Informationen über den Zustand der Systeme. Anhand der Meldungen kann sehr einfach und zuverlässig ein Ausfall vorhergesagt bzw. verhindert werden. Im Falle eines Ausfalls können wichtige Informationen für eine schnelle Behebung des Fehlers geliefert werden.

### Problem:

Derzeit gibt es keine einheitliche Schnittstelle zur Überwachung von Systemen. Diverse Protokolle (z.B. SNMP, Syslog, Eventlog, etc.) machen es den Administratoren schwer ein flächendeckendes Monitoring aufzubauen. Hinzu kommt die Fülle an Information. Systemkritische Ereignisse gehen oft in der Flut an Information unter.

### Beispiele:

1. Eine zu volle Festplatte in einem Datenbankserver führt unweigerlich zum anhalten der Datenbank. Im Eventlog des Servers steht zwar die Meldung der zu vollen Festplatte, der Administrator ist jedoch nicht in der Lage die Eventlogs aller 50 Server ständig im Auge zu behalten. Würde der Administrator z.B. per eMail oder SMS auf die langsam voller werdende Festplatte frühzeitig hingewiesen werden, könnte er rechtzeitig ein löschen von Daten veranlassen und das System bleiben ohne Unterbrechung verfügbar.
2. Oft werden Redundanzen bereits unbemerkt verwendet. So läuft z.B. ein RAID Server auch mit einer defekten Festplatte ohne spürbare Veränderung. Der Ausfall einer weiteren Platte führt jedoch unweigerlich zum Datenverlust. Wenn jetzt die Backups versagt haben, sind die Daten für immer verloren.

Derzeit wird in kleineren und mittelgroßen Umgebungen fast kein Monitoring durchgeführt. Der Zeitaufwand für die Installation und die Komplexität der Systeme sind zu hoch.

### Lösung:

#### indev:s ServerMonitoring (iSM):

Die indevis GmbH betreibt das Authentisierungssystem indevis SecurAccess (ISA) für Kunden. Dieser Dienst muss 100% verfügbar sein, 7 Tage die Woche, 24 Stunden, 365 Tage im Jahr. Um diese Verfügbarkeit zu erreichen wurde ein umfangreiches Web-basiertes Server-Monitoring sowie eine Netzwerküberwachung aufgebaut.

Unsere Erfahrungen mit diesen Systemen sind so positiv dass die indevis das Server-Monitoring nun auch Kunden für eine geringe monatliche Pauschale zu Verfügung stellt.

Selbstverständlich können nach einem erfolgreichen Test die Monitoring Appliances auch käuflich erworben werden und einen eigenständigen Einsatz in Ihrem Netzwerk finden.

### Wie funktioniert iSM?

Der Kunde nennt indevis die zu überwachenden Systeme (IP-Adressen). Mit den zuständigen Administratoren wird das Monitoring eingerichtet. Es werden nahezu alle IP-basierten Protokolle unterstützt. Das Monitoring erfolgt vom indevis iSM-Server aus - eine IP-Verbindung ist daher Voraussetzung für diese Dienstleistung.

Auf den zu überwachenden Servern muss zum Monitoring der Dienste ein „Monitoring Agent“ installiert werden. Der Agent kommuniziert dann auf einem festen IP-Port mit dem indevis ServerMonitoring (iSM) Server.

Die Alarmierung erfolgt über eMail oder SMS an die zuständigen Personen.

**iSM** kennt die Überwachungskette der Server, Router, Switches etc. So wird bei Ausfall des Internet-Routers nur dieser Router als Fehler gemeldet. Ein Monitoring der dahinterliegenden Server ist dann zwar nicht mehr möglich, solange der fehlerhafte Router nicht gewechselt wurde, wird aber kein weiterer Alarm ausgelöst.

Alle Informationen über den Zustand von angeschlossenen IT Systemen werden in einem System zusammengefasst und überwacht. Sie erhalten jederzeit einen Gesamtüberblick über die Leistungsfähigkeit Ihrer Ressourcen. Schwachpunkte lassen sich schon im Vorfeld erkennen und Sie optimieren langfristig die Verfügbarkeit Ihrer Systeme.

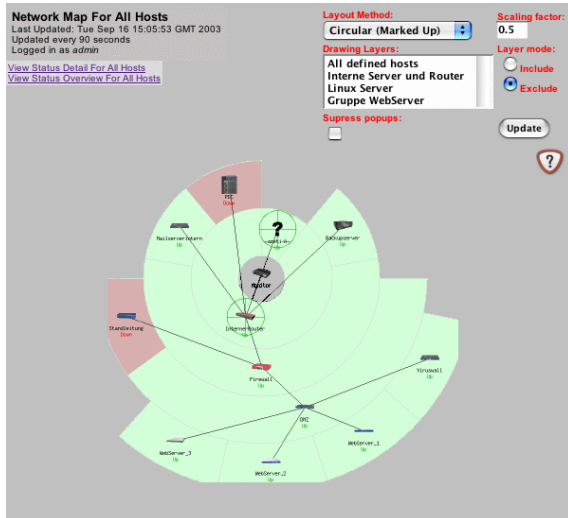


Abb.1: Vereinfachter Netzwerkplan



### Folgende Dienste können mit iSM überwacht werden:

[www.indevis.de/dokumente/indevis\\_monitoringdienste.pdf](http://www.indevis.de/dokumente/indevis_monitoringdienste.pdf)

### Wie informiert iSM?

Für jedes Ereignis kann individuell festgelegt werden, wie der Systemverantwortliche informiert wird. So reicht bei weniger wichtigen Ereignissen eine eMail. Bei systemkritischen Zuständen wird eine SMS auf ein Mobiltelefon gesendet. Im täglichen Betrieb kann sich der Administrator über eine Website alle Informationen zu den überwachten Systemen anzeigen lassen. Eine statistische Auswertung der Verfügbarkeit aller überwachten Dienste kann individuell erstellt werden.

### Technische Daten zu iSM:

Folgende Betriebssysteme und Produkte können mit iSM überwacht und monitored werden:

- MS Windows 2000 Server und NT
- Sun Solaris
- Linux
- Unix
- **Produkte die mit SNMP und TCP/IP arbeiten! (Server, Firewalls, Switches, Router, USV, etc.)**
- **Anwendungen wie Datenbanken, Fileserver, Drucker, Tools, etc.**
- **Netze wie VPNs, Festverbindungen, etc.**

### Weitere Daten zu iSM:

- Gehärtetes GNU Linux
- Keine Verschleißteile (Lüfter oder Festplatten)
- Automatische Netzwerkplan-Erstellung
- Benachrichtigt im Fehlerfall
- Automatische Backup-Funktion
- Automatische Update-Funktion

Wenn Sie Fragen zu indevis **ServerMonitoring (iSM)** haben stehen wir Ihnen jederzeit gerne unter Telefon +49 (89) 22 80 78 70 zur Verfügung.

**Gerne stellen wir Ihnen iSM für einen umfangreichen Test kostenlos zur Verfügung.**

Weitere Informationen zu indevis Server Monitoring finden Sie auf unserer Website [www.indevis.de](http://www.indevis.de).

Weitere Informationen zu unseren Produkten und Dienstleistungen finden Sie im Internet unter:

[www.indevis.de](http://www.indevis.de)