Technische Aspekte des Autonomic Computing
Oktober 2002

Tivoli software

Tivoli Software-Produkte und die IBM Autonomic Computing Initiative™

Tivoli Software: Intelligente IT-Management-Software, die integriert und automatisiert

Inhalt

Einleitung

Seit Jahrzehnten entwickelt die Hochtechnologiebranche Systeme zur Bewältigung vieler Problemstellungen in der Geschäftswelt. Diese Systeme werden immer komplizierter. Inzwischen ist diese Komplexität selbst zum Problem geworden. Nach der Inbetriebnahme eines Systems stellen sich mit der Zeit Hardware- und Softwareprobleme ein; Menschen machen Fehler, und Netzwerke wachsen und verändern sich. Verbesserungen und Veränderungen der Leistungsfähigkeit und Kapazität von IT-Komponenten erfordern oft ständiges menschliches Eingreifen. Ein System, das auf eine Reparatur oder sonstige Wartung wartet, verursacht unter Umständen erhebliche Kosten.

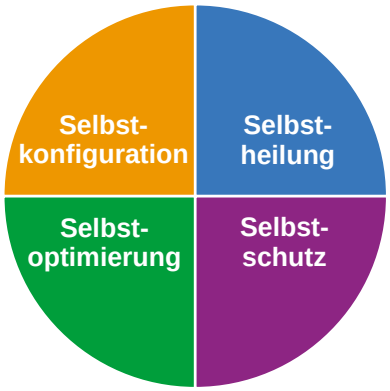
Angesichts der stringenten Kostensituation, in der sich viele Unternehmen befinden, kommt es für IT-Führungskräfte darauf an, den Return-on-Investment in ihrem Verantwortungsbereich zu steigern, indem sie die Gesamtkosten (Total Cost of Ownership, TCO) senken, gleichzeitig aber die Qualität ihrer Dienste verbessern und die Komplexität ihrer IT-Umgebung effizient verwalten.

Das Konzept des „Autonomic Computing“ zielt auf diese Problematik ab und zeichnet einen entsprechenden technologischen Weg des Technologie-Managements vor. Der englische Begriff „autonomic“ ist aus der Humanbiologie entlehnt. Die autonomen Systeme des menschlichen Körpers überwachen den Herzschlag, prüfen den Blutzuckerspiegel und halten die Körpertemperatur konstant auf 37°C, ohne dass sich der Mensch darum zu kümmern braucht; dementsprechend sieht das Autonomic Computing vor, dass bestimmte Systemkomponenten Erfordernisse vorausschauend erkennen und Probleme selbständig lösen, ohne dass der Mensch eingreift.

IBM Produkte mit autonomen Funktionen bergen in ihren prognostischen und vorausschauend agierenden Funktionen, die auf veränderte Umstände reagieren und Probleme vorwegnehmen, für Kunden ein erhebliches Wertschöpfungspotenzial. Das vorliegende Dokument definiert dieses Wertschöpfungspotenzial des Autonomic Computing und beschreibt die Voraussetzungen für die Herstellung einer autonomen Umgebung, die Schritte zu ihrer erfolgreichen Implementierung und die Produkte, mit denen sich dieses IT-Konzept realisieren lässt.

Wie profitiert der Kunde von Autonomic Computing?

Der Grundgedanke des Autonomic Computing ist die Reduzierung der Kosten und der Komplexität, die mit Besitz und Betrieb einer IT-Infrastruktur einhergehen. In einer „autonomen“ Umgebung verfügen die Komponenten der IT-Infrastruktur – vom Desktoprechner bis zum Mainframe – über vier Kerneigenschaften: Selbstkonfiguration, eigenständige Problembehebung („Selbstheilung“), Selbstoptimierung und Selbstschutz. Diese vier Attribute bilden das Fundament des Autonomic Computing.



Selbstkonfiguration
Durch die Fähigkeit, sich dynamisch im laufenden Betrieb selbst zu konfigurieren, kann sich eine IT-Infrastruktur – mit nur minimalem menschlichem Eingreifen – eigenständig auf die Eingliederung neuer Komponenten oder auf sonstige Veränderungen in der IT-Umgebung einstellen.

Selbstheilung
Eine „selbstheilende" IT-Infrastruktur kann das Ausfallen von IT-Komponenten erkennen und solche Ausfälle entweder beheben oder ihre Auswirkungen durch Umgehungsmaßnahmen abmildern, um die kontinuierliche Verfügbarkeit der Geschäftsanwendungen sicherzustellen.

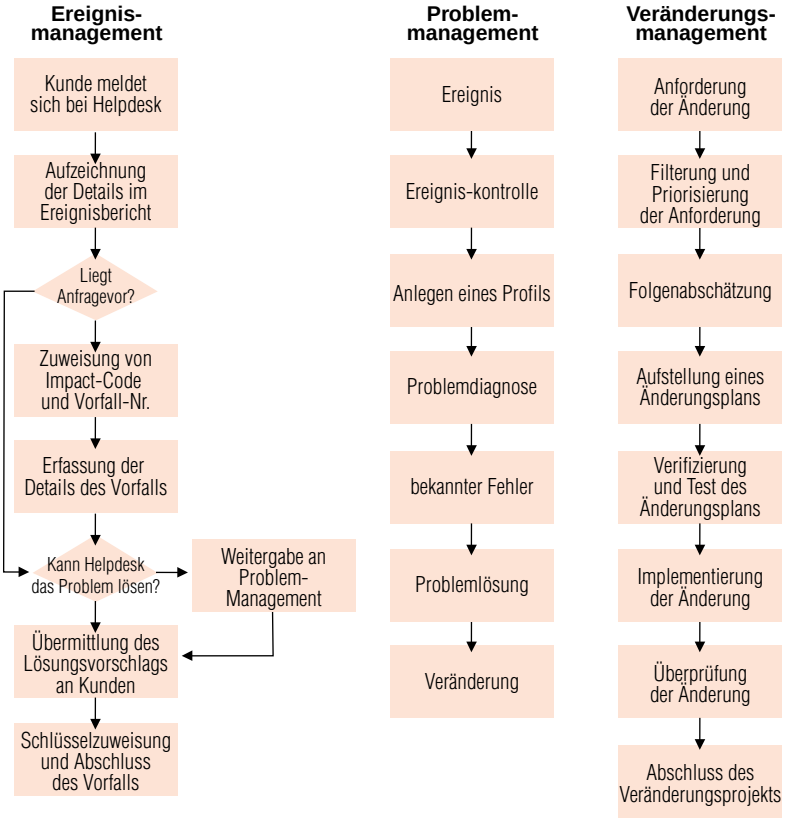
Selbstoptimierung
Selbstoptimierung ist die Fähigkeit einer IT-Umgebung, Ressourcen und ihre Nutzung unter minimalem menschlichem Eingreifen effizient zu verwalten.

Selbstschutz
Eine sich selbst schützende IT-Umgebung gewährleistet die effektive Verwaltung von Zugriffsrechten und kann automatisch geeignete Maßnahmen zur Reduzierung seiner Verwundbarkeit durch Angriffe auf die Laufzeit-Infrastruktur und die Geschäftsdaten treffen. Eine zum Selbstschutz fähige IT-Umgebung erkennt feindselige Verhaltensmuster und unbefugtes Eindringen („Intrusion") unmittelbar und trifft autonom Maßnahmen zu ihrem Schutz vor unbefugten Zu- und Eingriffen, Viren, Denial-of-Service-Angriffen und Ausfällen allgemeiner Art.

In einer autonomen Umgebung interagieren und kommunizieren die Komponenten miteinander und mit übergeordneten Management-Tools. Sie regulieren sich selbst und gegebenenfalls auch einander. Sie können das Netzwerk vorausschauend verwalten und die innere Komplexität dieser Aktivitäten vor dem Endanwender verbergen.

Die Verwirklichung des Autonomic Computing ist nach Auffassung von IBM mit der Aufgabe verknüpft, IBM Software zu automatischem Verhalten zu befähigen und IT-Infrastrukturen zu autonomem Systemmanagement zu befähigen, so dass die IT-Umgebung einschließlich der Systemmanagement-Software sich selbst konfigurieren, optimieren, reparieren und schützen kann.

In der Regel werden komplexe IT-Infrastrukturen durch eine Reihe von IT-Management-Prozessen verwaltet. Brancheninitiativen wie die IT Infrastructure Library und das IBM IT Process Model definieren entsprechende „Best Practices“. Das nachstehende Prozessdiagramm veranschaulicht an einem Beispiel, wie das Ereignis-, das Problem- und das Veränderungsmanagement im typischen Fall ablaufen. Die eigentlichen Mechanismen, die diesen Prozessen im gegebenen Fall zugrunde liegen, können von Umgebung zu Umgebung voneinander abweichen; die Grundfunktionalität bleibt jedoch meist gleich.



Effizienz und Effektivität dieser Prozesse werden in der Regel nach Messkriterien wie Zeitdauer, Prozentanteil der korrekt ausgeführten Transaktionen, erforderliche Qualifikationen, mittlere Ausführungskosten usw. beurteilt. Die Technologie des Autonomic Computing kann durch die Automatisierung von Teilschritten solcher Prozesse zur Verbesserung ihrer Effizienz und zu ihrer Beschleunigung beitragen.

Schnelle Prozessinitiierung. Im Normalfall müssen Prozesse dieser Art durch den Menschen ausgelöst werden (z.B. durch Erstellen der Änderungsanforderung, Erfassung der Details des Vorfalls, Öffnen eines Problemfall-Eintrags). Meist muss daher ein IT-Mitarbeiter Zeit für die Erfassung der benötigten Daten

aufwenden. In einem selbstverwalteten System können Systemkomponenten die Prozesse anhand von direkt aus dem System bezogenen Informationen auslösen. Dadurch wird der Arbeits- und Zeitaufwand für manuelle Eingaben in Reaktion auf relevante Ereignisse reduziert.

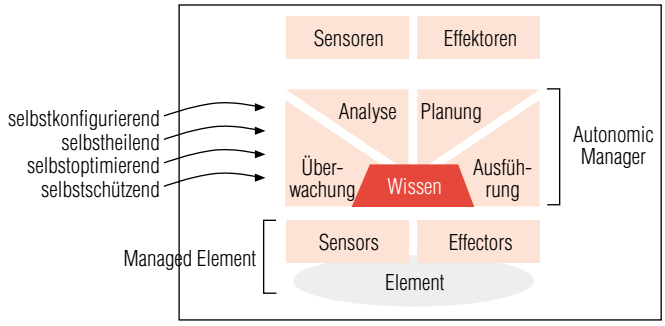
Geringere Anforderungen hinsichtlich Zeit und Qualifikation. Die Vorgänge und Maßnahmen im Verlauf dieser Prozesse erfordern meist eine hohe Qualifikation, dauern lange und sind beim ersten Mal aufgrund der Systemkomplexität kaum fehlerfrei auszuführen. Im Fall eines Veränderungsmanagement-Prozesses gilt dies beispielsweise für den Arbeitsgang „Impact-Analyse"; ein Beispiel aus dem Problem-Management wäre die Problemdiagnose. In selbstverwaltenden Systemen sind die Ressourcen so angelegt, dass die zur Durchführung dieser Arbeitsgänge erforderlichen Kenntnisse in das System integriert sind. Daher sind Zeitaufwand und Qualifikationsanforderungen wesentlich geringer.

Aufgrund ihrer Fähigkeit zur Selbstverwaltung kann die IT-Umgebung schneller reagieren; sie reduziert die Gesamtkosten und verkürzt die Zeit bis zur Wertschöpfung. Die Verringerung der Gesamtkosten ist der Tatsache zu verdanken, dass die IT-Mitarbeiter Prozesse zu niedrigeren durchschnittlichen Kosten ausführen können; die Wertschöpfung tritt früher ein, weil IT-Prozesse rascher ausgeführt werden.

In den nun folgenden Abschnitten werden die Technologie des Autonomic Computing und zu ihrer Realisierung geeignete Softwaretools beschrieben.

Architektonische Konzepte des Autonomic Computing

Die im untenstehenden Schema dargestellte Architektur nennt die architektonischen Elemente, aus denen sich eine autonome Umgebung zusammensetzt. Die Architektur besteht aus zwei Hauptelementen: einem verwalteten Teil („Managed Element") und einem autonomen Verwaltungsteil („Autonomic Manager").



Struktur von Selbstverwaltungstechnologien

Das verwaltete Element (Managed Element) ist die zu verwaltende Ressource. Auf dieser Ebene der Architektur kann es sich bei dem zu verwaltenden Element um eine Einzelressource oder auch eine Gruppe von Ressourcen (Ressourcenverbund) handeln. Das verwaltende Element (Management Element) exportiert „Sensoren“ und „Effektoren“. Sensoren sind Mechanismen zur Erfassung von Informationen über den Zustand bzw. Zustandsübergang eines Elements. Effektoren sind Mechanismen zum Ändern des Zustands eines Elements.

Sensoren und Effektoren bilden die instrumentelle Schnittstelle zum „Autonomic Manager“. Der Autonomic Manager implementiert den Regelkreis. Der Regelkreis beinhaltet in dieser Architektur vier Funktionen:

- ***Überwachung:*** *Mechanismen, die Detailaspekte eines Elements (Messkriterien, Topologien usw.) erfassen, sammeln, filtern, verwalten und melden.*
- ***Analyse:*** *Mechanismen, die komplexe Situationen korrelieren und modellieren (Zeitreihenvorhersage, Queuing-Modelle). Über diese Mechanismen kann der Autonomic Manager Erkenntnisse über die IT-Umgebung gewinnen und daraus folgernd zukünftige Situationen prognostizieren.*
- ***Planung.*** *Mechanismen zur Strukturierung der Maßnahmen, die zur Erreichung bestimmter Ziele nötig sind. Der Planungsmechanismus orientiert sich an Regeln.*
- ***Ausführung.*** *Mechanismen zur Ausführung eines Plans unter Einbeziehung von Aktualisierungen im Verarbeitungsverlauf.*

Die Funktionsbereiche Überwachung, Analyse, Planung und Ausführung des Autonomic Manager werden durch die Funktionalität der meisten IT-Prozesse abgedeckt. So sind zwar die Mechanismen und Details von IT-Prozessen wie Veränderungsmanagement und Problemmanagement unterschiedlich, jedoch lassen sich aus beiden vier gemeinsame Grundfunktionen abstrahieren: Erfassung der Fakten, Analyse der Fakten, Erstellung eines Aktionsplans und Ausführung des Plans. Diese vier Funktionen entsprechen den Komponenten Überwachung, Analyse, Planung und Ausführung unserer Architektur.

Die Mechanismen Analyse und Planung bilden den Kern eines autonomen IT-Systems; sie beinhalten das Know-how, das die Voraussetzung für die Reduzierung des Zeitaufwands und der erforderlichen Qualifikation des IT-Personals ist.

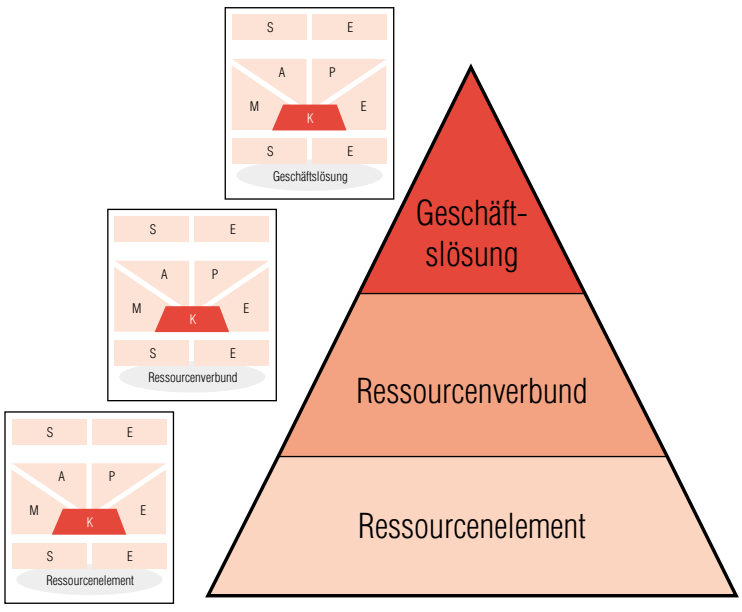
In dem mit „Wissen“ betitelten Bereich des Autonomic Manager werden die von dessen vier Komponenten benutzten Daten und Informationen gespeichert und bereitgestellt. Zu diesem Wissen gehören Regeln, topologische Informationen, Systemprotokolle und Leistungsmesskriterien.

Im Architekturschema ist eine zweite Gruppe von Sensoren und Effektoren vorgesehen. Diese ermöglichen die Kooperation mehrerer Autonomic Manager, die miteinander in einer Peer-to-Peer-Konstellation sowie mit übergeordneten Manager-Funktionen kommunizieren können.

Jedes Selbstverwaltungsmerkmal der Kernfunktionen Selbstkonfiguration, Selbstheilung, Selbstoptimierung und Selbstschutz ist als intelligenter Regelkreis (innerhalb eines Autonomic Managers) implementiert, der jeweils einen bestimmten operativen Aspekt der Konfiguration, Wiederinstandsetzung, Optimierung bzw. des Schutzes darstellt. So kann ein Autonomic Manager beispielsweise das System mit der richtigen Software selbständig neu konfigurieren, wenn Software ausfällt. Durch Erkennen eines ausgefallenen Elements kann er das System durch einen Neustart wieder instand setzen („heilen“). Wird eine erhöhte Kapazität erkannt, kann er die aktuelle Auslastung selbsttätig optimieren. Wird ein Eindringversuch festgestellt, kann er das System durch Abwehren des Angriffs im peripheren Bereich und durch Überprüfen der Ressource schützen.

Autonomic Computing in der IT-Umgebung

Um die Rolle des Autonomic Computing in verschiedenen Bereichen einer IT-Umgebung zu verstehen, muss man letztere auf verschiedenen Ebenen gesondert betrachten. Auf jeder dieser Ebenen bedingt das Selbstmanagement die Implementierung von Regelkreisen, mit deren Hilfe einzelne Ressourcen, Ressourcenverbunde und Geschäftslösungen Veränderungen ihrer Umgebung überwachen, analysieren, planen und ausführen können.



IBM bietet eine Serie von Management-Produkten an, die die Voraussetzungen für die Automatisierung von Management-Routinevorgängen einzelner Ressourcenelemente schaffen. IBM Produkte wie die Softwarefamilie IBM® Tivoli® Monitoring, IBM Tivoli Configuration Manager, IBM Tivoli Access Manager und IBM Tivoli Storage Manager bringen bereits Selbst-Management-Funktionalität für Ressourcenelemente (Systeme, Anwendungen, Middleware, Netzwerke und Speichergeräte) in die IT-Infrastruktur ein. Durch die IBM Server Group, die IBM Software Group und mehrere Drittanbieter setzt sich IBM für die Einbettung geeigneter Technologien und die Befähigung von Ressourcenelementen zur Teilnahme an einer autonomen IT-Infrastruktur ein.

Auf der Ressourcenverbund-Ebene ist die Entwicklung zum transaktionsgestützten Management der Schlüssel zum Autonomic Computing. In der Vergangenheit wurden Ressourcenelemente üblicherweise nach Typ (z.B. alle Server), Standort (z.B. alle Server innerhalb einer Abteilung oder Niederlassung) oder Funktion (z.B. alle Webserver) gruppiert. Im Zuge der Entwicklung von e-business-Umgebungen ist man dazu übergegangen, Ressourcen bevorzugt nach Transaktionskontext zu gruppieren, auch wenn es sich um verschiedenartige Ressourcen handelt. So werden beispielsweise Server, Anwendungen, Datenbanken und Speichereinrichtungen, die mit e-business-Transaktionen zu tun haben, separat von den für die Personalverwaltung zuständigen Ressourcen eingeordnet. Sowohl bei einem homogenen (z.B. Server-Cluster) als auch bei einem heterogenen Ressourcenverbund (z.B. Webserver, Datenbank und Speichersystem) bestimmen die Leistungs- und Verfügbarkeitsanforderungen verschiedener Transaktionsarten die autonomen Vorgänge in den einzelnen Ressourcenelementen. Um Service-Level-Vorgaben für IT-Transaktionen zu erfüllen, werden Ressourcen je nach Auslastung dynamisch zugewiesen, konfiguriert, optimiert sowie geschützt. IBM Tivoli Monitoring for Transaction Performance, IBM Tivoli Storage Resource Manager, IBM Tivoli Identity Director und Tivoli Configuration Manager sind Beispiele für IBM Produkte, die gemeinsam die Evolution des Autonomic Computing auf der Ressourcenverbund-Ebene vorantreiben.

Die höchste Schicht der IT-Umgebung bilden Geschäftslösungen, z.B. ein Kundenbetreuungssystem oder ein elektronisches Auktionssystem. Hier werden autonome Systemmanagementlösungen benötigt, die die Verarbeitungszustände von Geschäftsprozessen erkennen können – anhand von Regeln, Zeitplänen, Trends und Service-Level-Vorgaben sowie deren Konsequenzen – und die Transaktionssysteme und die ihnen untergeordneten Einzelressourcen zum entsprechenden Verhalten veranlassen. Solche Produkte mit „Geschäftssinn“ sind z.B. IBM Tivoli Service Level Advisor, IBM Tivoli Business Systems Manager und IBM Tivoli Systems Automation for S/390®.

Entwicklungsstufen des Autonomic Computing

Zur autonomen IT-Infrastruktur hin führt ein Evolutionsprozess, der durch Technologie vorangetrieben wird; die letztendliche Implementierung erfolgt unternehmensspezifisch durch Anwendung dieser Technologien und geeigneter Prozesse.

Das untenstehende Schema stellt diese Evolution einer IT-Umgebung bis zur uneingeschränkten Verwirklichung des autonomen Prinzips dar. Dabei werden die Phasen „Managed“, „Predictive“, „Adaptive“ und schließlich „Autonomic“ durchlaufen.

Basic Stufe 1	Managed Stufe 2	Predictive Stufe 3	Adaptive Stufe 4	Autonomic Stufe 5
• Mehrere Quellen system-generierter Daten • Erfordert umfangreichen, hochqualifizierten Mitarbeiterstab	• Datenkonsolidier-ung durch Management-Tools • IT-Mitarbeiter analysieren und handeln entsprechend • größere Systemtransparenz • erhöhte Produktivität	• System überwacht, korreliert und empfiehlt Maßnahmen • IT-Mitarbeiter prüfen/bestätigen und veranlassen Maßnahmen • Geringere Abhängigkeit von Hochqualifikationen • Schnelle, fundiertere Entscheidungs-prozesse	• System überwacht, korreliert und ergreift Maßnahmen • IT-Mitarbeiter verwalten Performance nach SLAs • Agile, robuste IT-Systeme, minimales menschliches Eingreifen	• Integrierte Komponenten werden anhand von Geschäftsregeln u. -vorschriften dynamisch verwaltet. • IT-Mitarbeiter setzen geschäftliche Anforderungen um • IT-Management wird durch Geschäftsregeln gesteuert • Wirtschaftliche Agilität und Widerstandsfähigkeit
manuell				autonom

1. Der Ausgangszustand „Basic Level“ entspricht der Beschaffenheit mancher heutiger IT-Umgebungen. Jedes Infrastrukturelement wird separat verwaltet und muss von IT-Mitarbeitern eingerichtet, überwacht und irgendwann auch ersetzt werden.

2. Auf der Stufe „Managed“ können mit Systemmanagement-Tools Informationen aus artverschiedenen Systemen erfasst und in einer begrenzten Anzahl von Konsolen zusammengefasst werden. Dadurch wird der Zeitaufwand, der bei zunehmen komplexer IT-Umgebung durch das Zusammentragen und Aufbereiten von Informationen durch den Administrator entsteht, reduziert.

3. Auf der Stufe „Predictive“ werden neue Technologien eingesetzt, um verschiedene Infrastrukturelemente korrelieren zu können. Diese Elemente sind ansatzweise in der Lage, Muster zu erkennen, die optimale Konfiguration vorherzusagen und dem Administrator Maßnahmen zu empfehlen.

4. Wenn sich diese Technologien entsprechend verbessert und die IT-Mitarbeiter sich an die Empfehlungen und die prognostische Leistungsfähigkeit dieser Systeme gewöhnt haben, kann die nächste Stufe („Adaptive Level“) anvisiert werden. Hier kann die IT-Umgebung automatisch Maßnahmen ergreifen. Dabei stützt sie sich auf die verfügbaren Informationen und die Kenntnis ihrer inneren Vorgänge.

5. Im vollständig autonomen Zustand wird der Betrieb der IT-Infrastruktur durch Geschäftsregeln und vorgegebene Ziele gesteuert. Die Anwender interagieren mit autonomen Tools, die Geschäftsprozesse überwachen und/oder Ziele anpassen.

In den nächsten Abschnitten werden die Entwicklungsstufen zum Autonomic Computing im Kontext der einzelnen Merkmale der Systemautonomie betrachtet: Selbstkonfiguration, Selbstheilung, Selbstoptimierung und Selbstschutz. Anhand dieser Beschreibungen können Sie die Entwicklungsstufe Ihrer eigenen Umgebung, die Leistungsfähigkeit der aktuellen Tools und das langfristige Potenzial Ihrer Umgebung beurteilen.

Selbstkonfiguration

Ein Unternehmen kann seine Reaktionsfähigkeit gegenüber Mitarbeitern und Kunden durch eine selbstkonfigurierende IT-Umgebung wesentlich steigern. Ist eine IT-Infrastruktur in der Lage, sich dynamisch im laufenden Betrieb selbst zu konfigurieren, kann sie sich – mit nur minimalem menschlichem Eingreifen – sofort selbständig auf die Eingliederung neuer Komponenten oder auf sonstige Veränderungen in der IT-Umgebung einstellen. So kann sich beispielsweise ein e-business-Einzelhandelsunternehmen auf Stoßzeiten während der Vorweihnachtszeit oder vor sonstigen Ereignissen einstellen, indem es eine selbstkonfigurierende IT-Umgebung aufbaut, die Server aus nicht ausgelasteten Pools umwidmet und je nach Bedarf zur Entlastung der überbeanspruchten Server heranzieht. Tivoli Software-Management-Tools von IBM erschließen eine Vielzahl von Ressourcen – Systeme, Anwendungen, Nutzer- und Zugriffsrechte sowie physische und logische Speicherkapazitäten. Überwachungs- und Ereigniskorrelationstools helfen festzustellen, wann Veränderungen der IT-Infrastruktur Umkonfigurationsmaßnahmen erfordern. Mit diesen Tools lässt sich eine IT-Umgebung in Minuten oder Stunden anstatt in Tagen oder Wochen neu konfigurieren.

IBM hat – ausgehend von den wichtigsten Voraussetzungen einer wirklich autonomen Funktionalität – fünf Implementierungsstufen für selbstkonfigurierende IT-Infrastrukturen definiert:

Basic **Stufe 1**	**Managed** **Stufe 2**	**Predictive** **Stufe 3**	**Adaptive** **Stufe 4**	**Autonomic** **Stufe 5**
Definition • Konfiguration, Optimierung, Instandsetzung und Schutz einzelner IT-Komponenten erfolgen anhand von Systemberichten, Produkt-Dokumentationen und manuellen Eingriffen. • Alle Maßnahmen erfordern menschliches Eingreifen	**Definition** • Software überwacht, konsolidiert, erleichtert und automatisiert manche IT-Aufgaben • Belastungsausgleich durch Cluster möglich • IT-Personal führt Analysen und Maßnahmen durch	**Definition** • Einzelne IT-Komponenten und Systemtools überwachen und analysieren Veränderungen • Anwender- und rollen-abhängige Ressourcenumwidmung • Kapazitäts-regelung auf Ressourcenebene zur Förderung der Transaktionsleistung	**Definition** • IT-Komponenten überwachen, analysieren und handeln einzeln und im Verbund unter minimalem menschlichem Eingreifen. • IT-Regeln bestimmen Kapazitätszuweisung über mehrere spezifische Ressourcenarten hinweg	**Definition** • IT-Komponenten werden kollektiv und automatisch durch in das System eingebettete Geschäfts-regeln verwaltet. • Ressource-nerkennung und Umwidmung von Kapazitäten
Vorteile Systeme werden einzeln konfiguriert und verwaltet.	**Vorteile** Höhere Produktivität von Administratoren durch schnelle Systeminstallation	**Vorteile** Fördert administrative Produktivität durch rollenorientierte Bereitstellung	**Vorteile** Höhere Systemverfüg-barkeit, geringere Intervention durch Menschen dank ereignisorientierter automatischer Bereitstellung	**Vorteile** Optimierung der Geschäfts-ressourcen nach Maßgabe von Servicestufen und geschäftlichen Prioritäten

Stufe 1: Basic
Das Augenmerk liegt auf der Bereitstellung, Konfiguration und Veränderbarkeit einzelner Systemkomponenten, d.h. Konfiguration von Systemhardware, Speicherhardware, Kommunikation und Betriebssystem. Zur Konfiguration werden einfache, ressourcenspezifische Tools eingesetzt. Die Konfiguration mehrerer Ressourcen erfolgt durch separates Anmelden beim Administrator-Tool jeder einzelnen Ressource zu deren Konfiguration.

Stufe 2: Managed
Im Zentrum steht die Fähigkeit zur Bereitstellung und zum Veränderungsmanagement einer Gruppe zusammengehöriger Systeme. Es werden mehrere Systeme und Systemabbilder verwaltet, Systeme werde in

Cluster eingegliedert oder daraus entnommen, Anwendungen werden für Gruppen von Rechnern bereitgestellt, Benutzergruppen werden verwaltet, und Speichereinheiten werden in Speichernetzwerke ein- und daraus ausgegliedert. Das Konzept der „Virtualized Storage“ wird eingeführt; die kollektive Überwachung des Systemzustands und der Speicherkomponenten wird erwogen, um fundierte Entscheidungen über deren Neuzuweisung und Umkonfiguration fällen zu können.

Stufe 3: Predictive
Das Konzept des rollenorientierten Managements wird eingeführt, zu dem Benutzer- und Systemrollen gehören; dadurch sind zweckbestimmte Konfigurationen möglich. Anhand von Konfigurationserkennung (z.B. Inventarabfrage) und Laufzeitüberwachung wird entschieden, wann Korrekturmaßnahmen erforderlich sind. Der Administrator kann solche Maßnahmen aufgrund von Empfehlungen des Systems auslösen.

Stufe 4: Adaptive
Im Blickpunkt liegt das dynamische Management der Umgebungskonfiguration durch leistungsfähige Korrelation und Automatisierung. Das zentrale Interesse liegt in der automatischen Umkonfiguration und der Selbstregulierung der IT-Infrastruktur je nach dem Gesamtzustand der Konfiguration sowie nach Rollenveränderungen.

Stufe 5: Autonomic
Umkonfigurationen erfolgen im Kontext allgemeiner Geschäftsregeln und Prioritäten. Die erforderlichen Umkonfigurationsmaßnahmen werden durch Business-Impact-Analyse ermittelt. Außerdem können vorbeugende Maßnahmen getroffen und mögliche Gefährdungen der Servicestufen vor ihrem tatsächlichen Eintreten erkannt und abgewendet werden.

Selbstkonfiguration durch Tivoli Softwareprodukte

Folgende Tivoli Softwareprodukte eignen sich zur Implementierung einer selbstkonfigurierenden Umgebung:

IBM Tivoli Configuration Manager
IBM Tivoli Configuration Manager führt automatisch Neukonfigurationen in sich rasch verändernden Umgebungen durch. Ein Inventarabfrage-Engine und ein Zustandsmanagement-Engine können erkennen, wann Software in einem Zielsystem nicht mehr dem Referenzmodell für die betreffende Systemklasse entspricht. IBM Tivoli Configuration Manager kann automatisch für jedes Ziel einen speziellen Bereitstellungsplan generieren und die Installation der Software in der richtigen Reihenfolge vornehmen.

IBM Tivoli Identity Manager
IBM Tivoli Identity Manager automatisiert das Benutzer-Lifecycle-Management und lässt sich an Personal- sowie native Repositorien anbinden. Das Anlegen von Konten erfolgt nach automatischen, rollenorientierten Regeln. Das Bereitstellungssystem kommuniziert beim Anlegen von Konten, bei der Lieferung von Benutzerinformationen und Passwörtern und der Definition von Kontoberechtigungen direkt mit den Zugangssteuerungssystemen.

IBM Tivoli Storage Manager
IBM Tivoli Storage Manager besitzt Selbstkonfigurationsfunktionen für Aufgaben wie das automatische Identifizieren und Laden der richtigen Treiber für die am Server angeschlossenen Speichergeräte. Konfigurationsinformationen und Regeln brauchen nur einmal in einem Tivoli Storage Manager-Konfigurationsserver definiert zu werden und können dann an mehrere verwaltete Tivoli Storage Manager-Server weitergeleitet werden. Regeln und interne Automatismen ermöglichen die automatische Erweiterung der Serverdatenbank und/oder des Wiederherstellungsprotokolls bei Erreichen der vom Administrator festgelegten Schwellwerte.

Selbstheilung

Eine „selbstheilende“ IT-Infrastruktur kann Abweichungen vom Normalbetrieb von Systemen, Transaktionen und Geschäftsprozessen vorausschauend oder reagierend erkennen und ohne Benutzerintervention Korrekturmaßnahmen auslösen. Eine Korrekturmaßnahme kann beispielsweise darin bestehen, dass eine Komponente verändert wird oder andere Komponenten so angepasst werden, dass sie die Aufgabe einer ausgefallenen Komponente übernehmen können. Der tägliche Betrieb wird durch Vorfälle auf Komponentenebene nicht beeinträchtigt oder unterbrochen. Das Angebot an IBM Tivoli Software-Management-Produkten besteht aus Tools, mit deren Hilfe Kunden den Zustand und die Performance ihrer IT-Infrastruktur überwachen können. Die Überwachung kann mehrere Messkriterien umfassen und sich auf heterogene Ressourcen erstrecken; erfasste Daten können gefiltert, korreliert und analysiert werden. Ausgehend von der Analyse können automatisch Maßnahmen zur Behebung potenzieller Probleme ausgelöst werden. Autonome Funktionen auf mehreren Ebenen ermöglichen dem Kunden die Abschätzung geschäftlicher Auswirkungen sowie ein vorausschauendes Verfügbarkeitsmanagement der IT-Infrastruktur. Workbench-Tools gestatten die Einbindung der Anwendungen von Drittherstellern.

IBM hat – ausgehend von den wichtigsten Voraussetzungen einer wirklich autonomen Funktionalität – fünf Implementierungsstufen für Selbstheilung und Verfügbarkeitsmanagement definiert:

Basic Stufe 1	Managed Stufe 2	Predictive Stufe 3	Adaptive Stufe 4	Autonomic Stufe 5
Definition • Jedes System besitzt eigene lokale Adminis-trationskonsole • Problem-untersuchung meist durch Lesen von Protokollen durch Personal • IT-Verfügbark-eitsberichte werden manuell erstellt	**Definition** • Zentrale Über-wachung von und Berichters-tattung über IT-Ressourcen • Zentraler Einsatz von Produkten für Filterung, Korrelation und Management von Ereignissen • Manuelle Problembehebung durch qualifizierte Administratoren	**Definition** • Überwachung und Prognose der durch IT-Ressourcen bedingten Transak-tionsverzögerungen • Business-Impact von Ressourcen-problemen ist nachvollziehbar • Automatische Abhilfema-ßnahmen bei Routineproblemen möglich	**Definition** • Regelorientierte, auf Sollzustand ausgerichtete Infrastruktur stellt Funktionsfähigkeit selbsttätig wiederher. • Erkennung und automatische Korrektur problematischer Trends	**Definition** • Dynamische Wiederbereitstellung der IT-Infrastruktur bei Ressource-nausfall • Automatische Gewährleistung der Geschäfts-kontinuität
Value Trägt zur Verring-erung der Ausgaben im IT-Bereich bei.	**Value** Helps increase ROI of IT resources and IT services	**Value** IT-Ressourcen werden im geschäftlichen Kontext verwaltet.	**Value** Steigerung der Geschäftsver-fügbarkeit	**Value** Optimaler positiver Geschäfts-beitrag der IT-Dienste

Stufe 1: Basic
Systemadministration und Problembehandlung erfolgen im Wesentlichen durch den Menschen. Die Systemverfügbarkeit wird reagierend gehandhabt. Die Unterrichtung der IT-Abteilung über Probleme erfolgt durch Kunden, die sich über Dienstausfälle beschweren. Die Problemidentifizierung, -korrelation und -behebung erfordert umfangreiche menschliche Intervention. Zum Beheben von Problemen werden hochqualifizierte IT-Mitarbeiter benötigt.

Stufe 2: Managed
Der Schwerpunkt liegt auf der Erfassung von und Einsichtnahme in Verfügbarkeitsinformationen von entfernten Standorten. Viele Ressourcen sind ggf. außerhalb des Rechenzentrums angesiedelt, z.B. in Zweigstellen. Fehlerprotokolle sind entfernt zugreifbar. Die IT-Abteilung hat

Überwachungstools installiert, die Berichte über die Verfügbarkeit an einen zentralen Standort liefern. System- und Netzwerkereignisse können gefiltert oder manuell korreliert werden, um die Grundursachen von Problemen ausfindig zu machen. Probleme werden durch qualifizierte Administratoren manuell behoben.

Stufe 3: Predictive
Die IT-Administration verfügt über Einblicke von hohem Auflösungsvermögen in die IT-Systeme und kann daher Ausfallursachen genau lokalisieren. An die Stelle einzelner, ressourcenspezifischer Messverfahren treten komplexe, viele Parameter umfassende Möglichkeiten der Messdatenerhebung. Leistungsfähige Filterfunktionen und Korrelations-Engines ermöglichen eine Grundursachenermittlung auf hohem Niveau. Bekannte Probleme können automatisch behoben werden. Dank dieser Funktionalität kann der Kunde die Problembehebung je nach Relevanz für den Geschäftsbetrieb priorisieren.

Stufe 4: Adaptive
IT-Systeme können Probleme in einer Vielzahl von überwachten Ressourcen (Betriebssystem, Anwendungen, Middleware) automatisch erkennen, diagnostizieren und beheben. Die Verfügbarkeit der Infrastruktur wird automatisch sichergestellt und orientiert sich an definierten Sollzuständen. Ausfälle kompromittieren das Gesamtsystem nicht, da dieses dynamisch Kompensationsmaßnahmen trifft, bis entsprechende Reparaturen möglich sind. Die Aufrechterhaltung der Servicestufen ist somit gewährleistet. Bei erhöhter Belastung werden beispielsweise die Schwellwerte vorübergehend erhöht.

Stufe 5: Autonomic
Die Problemerkennung und -diagnose beruht auf detailliertem Wissen über Komponenten und ihre Wechselbeziehungen, das bereits in das System eingebettet ist. Das System ist in der Lage, durch Schlussfolgerung automatisch innerhalb des vorgegebenen geschäftlichen Rahmens Korrekturmaßnahmen zu generieren. Kann beispielsweise ein bestimmter Ausfall nicht mit den verfügbaren Ressourcen kompensiert werden, werden Geschäftsanwendungen niedriger Priorität heruntergefahren oder auf niedrigerem Dienstqualitätsniveau weiterbetrieben, um die Funktionsfähigkeit wichtiger Geschäftsanwendungen zu sichern.

Systemselbstheilung durch Tivoli Softwareprodukte
Folgende Tivoli Softwareprodukte eignen sich zur Implementierung einer selbstheilenden Umgebung:

IBM Tivoli Enterprise Console
IBM Tivoli Enterprise Console® sortiert und bündelt Fehlerberichte, schließt auf die Grundursachen und löst Korrekturmaßnahmen aus. Der Ereignisserver und der Korrelations-Engine ermöglichen die ressourcenübergreifende Korrelation von beobachteten Vorfällen in Hardware, Anwendungen und Netzwerkgeräten des gesamten Unternehmens. Ereignisse aus vielen Ressourcen können in Echtzeit analysiert werden, um automatisch die wirklich kritischen Probleme zu ermitteln und von irreführenden Symptomen und Effekten zu unterscheiden. Nachdem ein Problem isoliert worden ist, ergreift das System Maßnahmen zur Problembehebung, indem es entweder automatisch reagiert, sofern dies möglich ist, oder die Support-Mitarbeiter zu geeigneten Eingriffen anleitet.

IBM Tivoli Switch Analyzer
IBM Tivoli Switch Analyzer korreliert Netzwerkgerätefehler ohne Nutzerintervention mit den Grundursachen. Als Layer-2-Schalter-Netzwerkmanagementlösung erkennt das Produkt automatisch Layer-2-Geräte. Es identifiziert Beziehungen zwischen Geräten einschließlich Layer-2- und Layer-3-Geräten und bestimmt die Grundursachen von Problemen ohne menschliches Eingreifen. Bei gleichzeitigem Eintritt einer größeren Anzahl von Ereignissen kann es wichtige von unwichtigen Vorfällen unterscheiden und die tatsächliche Ursache des Problems bestimmen.

IBM Tivoli NetView
IBM Tivoli NetView® schafft Möglichkeiten der automatischen Reparatur durch Erkennung von TCP/IP-Netzwerken, Darstellen von Netzwerktopologien, Korrelieren und Verwalten von Ereignissen und SNMP-Fehlerquellen, Überwachen des Netzwerkzustandes und Erfassen von Performance-Daten. Durch Router-Fehlereingrenzungstechnologie werden Ursachen von Netzwerkfehlern rasch ermittelt, gezielt behandelt und durch Korrekturmaßnahmen behoben.

IBM Tivoli Business Systems Manager
IBM Tivoli Business Systems Manager erfasst Echtzeit-Betriebsdaten von verteilten Anwendungskomponenten und Ressourcen aus dem gesamten Unternehmen und liefert eine umfassende Sicht der IT-Infrastruktur-komponenten, aus denen sich verschiedene Geschäftslösungen zusammensetzen. Es beinhaltet Analysetechnologien, die ermitteln können, wie sich ein Ausfall auf einen Geschäftsbereich, einen wichtigen Geschäftsprozess oder ein Service-Level-Agreement (SLA) auswirken würde.

IBM Tivoli Systems Automation S/390
IBM Tivoli Systems Automation S/390 verwaltet Echtzeit-Probleme im Kontext der geschäftlichen Prioritäten des Unternehmens. Es überwacht und verwaltet essenzielle Systemressourcen wie Prozessoren, Untersysteme, Sysplex-Timer und Kopplungseinrichtungen. Es unterstützt die eigenständige Systemreparatur durch Mechanismen zur Umkonfiguration der Partitionen eines Prozessors, zum Zurückstellen von IML-Prozessoren und IPL-Betriebssystemen beim Einschalten (auch automatisch), zur Untersuchung von und Reaktion auf E/A-Konfigurationsfehler sowie zum Neustarten und Stoppen von Anwendungen im Störungsfall.

IBM Tivoli Risk Manager
IBM Tivoli Risk Manager schafft Voraussetzungen für die automatische Selbstreparatur durch Auswerten möglicher Sicherheitsbedrohungen und automatisches Einleiten von Gegenmaßnahmen, z.B. durch Server-Umkonfiguration, Implementierung von Security-Patches und Zwangsschließung von Zugangskonten. Dadurch können auch Systemadministratoren, die nicht über Expertenkenntnisse im Security-Bereich verfügen, die zahlreichen möglichen Angriffsziele im gesamten Unternehmen in Echtzeit und mit einem hohen Maß an Integrität und Treffsicherheit auf Sicherheitsrisiken überwachen und diese Risiken einschätzen. Dieses Produkt ist mit Technologie von IBM Research ausgestattet.

IBM Tivoli Monitoring for Applications, IBM Tivoli Monitoring for Databases und IBM Tivoli Monitoring for Web Infrastructure
Diese Produkte reduzieren die Verwundbarkeit von Systemen auf ein Minimum, indem sie Unterbrechungen erkennen, diagnostizieren und automatisch darauf reagieren. Diese Produktfamilie umfasst Überwachungslösungen und lokale Automatisierungsfunktionen auf der Basis vorausschauender Analyse-Komponenten (Proactive Analysis Components). Ein hochentwickelter Ressourcenmodell-Engine ermöglicht die lokale Filterung von Überwachungsdaten und signalisiert unter bestimmten Bedingungen ein Ereignis. Durch Implementieren lokaler Regeln können sofortige Korrekturmaßnahmen veranlasst werden, so dass bei Serverausfällen eine automatische Systemwiederherstellung durchgeführt wird..

IBM Tivoli Storage Resource Manager
IBM Tivoli Storage Resource Manager erkennt automatisch potenzielle Probleme und führt regelgestützte Maßnahmen aus, um Speicherprobleme zu verhindern bzw. zu lösen, die Kosten der Speicherung zu reduzieren und die Verfügbarkeit von Anwendungen sicherzustellen. Es kann Speicherressourcen abfragen und in der IT-Umgebung erkennen. Es unterstützt die regelgestützte Automatisierung der Zuweisung von Speicherquoten und Speicherplatz, überwacht Dateisysteme und erstellt Berichte über Speicherkapazitäten und Speicherbelegung.

Selbstoptimierung

Selbstoptimierung ist die Fähigkeit der IT-Infrastruktur, durch eine effiziente, optimierte Ressourcenzuweisung und Ressourcennutzung eine hohe Dienstqualität für die Nutzer des Systems und ihre Kunden sicherzustellen. Zunächst betrifft die Selbstoptimierung vorwiegend die Komplexität des Systemleistungsmanagements. Langfristig sollen selbstoptimierende Softwareprodukte aus Erfahrung lernen und sich selbst vorausschauend auf die Geschäftsziele abstimmen können. Das Workload-Management nutzt Selbstoptimierungstechnologie zur Optimierung der Hardware- und Softwareauslastung und zur Verifizierung der Erfüllung von Servicestufen-Vorgaben. Prognos-tizierende Analyse-Tools geben Einblicke in Leistungstrends und ermöglichen vorbeugende Maßnahmen zur Optimierung der IT-Infrastruktur, bevor kritische Schwellwerte überschritten werden.

IBM hat fünf Implementierungsstufen für selbstoptimierende IT-Infrastrukturen definiert, die die Systemauslastung und die Transaktionsleistung ressourcenübergreifend optimieren können:

Basic **Stufe 1**	**Managed** **Stufe 2**	**Predictive** **Stufe 3**	**Adaptive** **Stufe 4**	**Autonomic** **Stufe 5**
Definition • Überwachung von und Berichterstattung über die Performance einzelner IT-Ressourcen, allerdings in inkompatiblen Formaten • Manuelle Optimierung der Leistung einzelner IT-Ressourcen	**Definition** • Überwachung von und Berichterstattung über die Performance aus Sicht des Anwenders (Transaktionen) • Zentralisierte, umfassende Sicht der Performance • Manuelle Optimierung von Gruppen aus verbundenen Ressourcen	**Definition** • Implementierung und Verwaltung von Service-Level-Agreements und Prioritäten • Service-Levels in Echtzeit sichtbar; prognostische Darstellung • Analyse und Empfehlungen zur manuellen Optimierung	**Definition** • Regelgestützt, sollzustandsorientiert • Service-Level-Prioritäten steuern automatische [Um-] Konfiguration und regeln Auslastung entsprechend den Zielvorgaben • Automatische Ressourcen-abstimmung durch Regelkreise	**Definition** • Dynamische Bereitstellung von Teilen der IT-Infrastruktur je nach Auslastungsgrad und Service-Level-Vorgaben • Automatische Transaktions-abstimmung durch Regelkreise
Value Verringerung der Ausgaben im IT-Bereich	**Value** Höherer ROI aus IT-Ressourcen und IT-Diensten	**Value** Leistung und Wertschöpfung von IT-Diensten sind prognostizierbar	**Value** Flexibilität; rasche Betriebs-bereitschaft neuer IT-Dienste	**Value** Optimaler positiver Geschäfts-beitrag der IT-Dienste

Stufe 1: Basic
Einzelne Ressourcen liefern punktuelle Daten zu ihrer Leistung und Nutzung und bieten dem Nutzer eine einfache Sicht der Auslastung von Einzelsystemen. Einfache Tools gestatten eine dynamische Darstellung von Komponenten; umfassende Darstellungen der Systemleistung müssen durch Auswerten zahlreicher lokaler Darstellungen und Berichte aus ressourcenspezifischen Tools manuell zusammengestellt werden.

Stufe 2: Managed
Mit Management-Tools können Daten zur Ressourcennutzung und -leistung erfasst und an einem zentralen Ort zusammengetragen werden. Einfache, umfassende Transaktionsdarstellungen sind möglich; sie beruhen auf Verfahren wie Zweirichtungsmessung, Testtransaktionen und Performancedatenerfassung aus einzelnen Arbeitsstationen. Viele Ressourcen, die sich in der Mitte des Transaktionsweges befinden, sind nicht sichtbar oder nicht instrumentiert; andere Ressourcen sind an Standorten außerhalb des Rechenzentrums untergebracht, z.B. in Zweigstellen. Die Optimierung von IT-Komponenten erfolgt manuell, oft nach dem „Trial-and-Error"-Prinzip.

Stufe 3: Predictive
Management-Tools wirken wertschöpfend, indem sie detaillierte, umfassende Transaktionsdarstellungen erstellen und die Gesamtsicht einer Transaktion nach Ressourcenelementen aufschlüsseln können. Ressourcen lassen sich nach Transaktionsarten gruppieren, Servicestufen können überwacht werden, und automatische Tools weisen auf drohende Regelverletzungen hin, woraufhin die IT-Umgebung manuell umkonfiguriert werden kann. Prognose-Tools liefern Trendanalysen anhand historischer Daten und geben Empfehlungen.

Stufe 4: Adaptive
Ressourcenverbunde sind instrumentiert und gestatten dadurch Zustandsänderungen sowie einen automatischen Belastungsausgleich bei Überlastung oder Unterbeanspruchung der Ressourcen in der Umgebung. Auf dieser Stufe hat der Nutzer weit reichende Möglichkeiten der Performance-Steuerung und kann die Vorgaben von SLAs effektiv erfüllen.

Stufe 5: Autonomic
Belastungsausgleich und Transaktionsoptimierung orientieren sich an den geschäftlichen Erfordernissen. Geschäftliche Alternativen werden in elektronisch verarbeitbarer Form ausgedrückt, so dass IT-Management-Tools Ressourcen den veränderlichen geschäftlichen Anforderungen entsprechend dynamisch zuweisen können. Durch automatische Feinabstimmung von Servern, Speichergeräten und Netzwerken wird die für die essenziellen Geschäftsanwendungen benötigte Dienstqualität sichergestellt.

Systemselbstoptimierung durch Tivoli Softwareprodukte
Folgende Tivoli Softwareprodukte eignen sich zur Implementierung einer selbstoptimierenden Umgebung:

IBM Tivoli Service Level Advisor
IBM Tivoli Service Level Advisor verhindert SLA-Verletzungen und verfügt über Prognosefunktionen. Es führt Trendanalysen an historischen Performance-Daten aus dem Tivoli Enterprise™ Data Warehouse durch und kann drohende Überschreitungen kritischer Schwellwerte vorhersagen. Durch Signalisieren eines Ereignisses an Tivoli Enterprise Console können Selbstoptimierungsmaßnahmen veranlasst werden, um das Wiederauftreten des Problems zu verhindern.

IBM Tivoli Workload Scheduler for Applications
IBM Tivoli Workload Scheduler for Applications automatisiert, überwacht und steuert die Transaktionsströme durch die IT-Infrastruktur sowohl in lokalen als auch entfernten Systemen. Es kann ihre Verarbeitung den vorliegenden Geschäftsregeln entsprechend automatisieren, planen und steuern. Anhand spezieller Algorithmen sorgt es für einen maximalen Transaktionsdurchsatz und trägt zur Optimierung der Ressourcennutzung bei.

IBM Tivoli Business Systems Manager
IBM Tivoli Business Systems Manager dient zur Optimierung der Behebung von IT-Problemen je nach den zu erwartenden geschäftlichen Auswirkungen von Ausfällen. Es erfasst Echtzeit-Betriebsdaten von verteilten Anwendungskomponenten und Ressourcen aus dem gesamten Unternehmen und liefert eine umfassende Sicht der IT-Infrastrukturkomponenten, aus denen sich verschiedene Geschäftslösungen zusammensetzen. Gemeinsam mit Tivoli Enterprise Console veranlasst es Maßnahmen zur Selbstoptimierung, um zu verhindern, dass Geschäftsbereiche, essenzielle Geschäftsprozesse oder SLAs durch Performance-Mängel beeinträchtigt werden.

IBM Tivoli Storage Manager
IBM Tivoli Storage Manager verbessert die Ressourcennutzung bei der Datensicherung unter Anwendung des Adaptive-Differencing-Prinzips. Durch Adaptive Differencing kann der Datensicherungs- und Archivierungs-Client dynamisch entscheiden, welches Verfahren zur Anfertigung von Sicherungskopien am effizientesten ist: die Sicherung der veränderten Bytes, der veränderten Datensätze oder der veränderten Dateien. Dadurch wird die Datensicherung über Einwahlverbindungen wesentlich effizienter. Diese Technologie bewirkt, dass bei der Datensicherung jeweils die geringstmögliche Datenmenge übertragen wird, und erzielt so die geringstmögliche Beanspruchung der Netzwerkbandbreite, der Speicherbänder sowie der Verwaltungsressourcen.

IBM Tivoli Monitoring for Transaction Performance
IBM Tivoli Monitoring for Transaction Performance ermöglicht die Abstimmung der IT-Umgebung entsprechend den Vorgaben der Servicestufen. Es überwacht die Leistung und Verfügbarkeit von e-business- und sonstigen Geschäftstransaktionen und sorgt dafür, dass der kommunizierende Kunde einen ungetrübt positiven Eindruck erhält. Zur Unterstützung der Warnfunktionalität und des vorausschauenden Managements verfügt es über eine Anbindung an die Tivoli-Enterprise-Console-Umgebung und trägt zur Optimierung der Ressourcennutzung aus der Transaktionsperspektive bei.

IBM Tivoli Analyzer for Lotus Domino
IBM Tivoli Analyzer for Lotus® Domino™ besitzt eine vorausschauende Analysekomponente, mit deren Hilfe Administratoren die Verfügbarkeit und optimale Performance von Lotus-Domino-Servern nachprüfen können. Es bietet intelligente Server-Zustandsüberwachungsfunktionen und liefert präzise Empfehlungen zur Problembeseitigung.

Selbstschutz

Eine sich selbst schützende IT-Umgebung kann automatisch Maßnahmen einleiten, um ihre Anfälligkeit gegen Angriffe auf ihre Laufzeitinfrastruktur und ihre Geschäftsdaten zu verringern. Solche Angriffe können in Form unbefugten Zugriffs oder unautorisierter Nutzung, als Virusattacken, die Festplatten formatieren und Geschäftsdaten zerstören, oder als Denial-of-Service-Angriffe erfolgen, die wichtige Geschäftsanwendungen lahm legen. Um alle diese Bedrohungen abzuwehren, ist eine Kombination von Security-Management- und Speichermanagement-Tools notwendig. Security-Management-Tools schaffen die Voraussetzungen für die konsequente Umsetzung von Sicherheits- und Datenschutzregeln; sie tragen zur Senkung der Administrationskosten im Security-Bereich bei, und sie steigern die Mitarbeiterproduktivität und die Kundenzufriedenheit. Schwerwiegende Konfigurationsänderungen sowie Änderungen der Zugangsverwaltung müssen eine entsprechende Autorisierung voraussetzen. Verletzungen von Sicherheitsregeln müssen durch geeignete Tools erkannt werden; erforderlichenfalls müssen automatisch Maßnahmen zur Minimierung des Risikos für IT-Sachwerte eingeleitet werden. Mit Speichermanagement-Tools von Tivoli Software können Unternehmen ihre Geschäftsdaten automatisch und effizient sichern und schützen. Autonome Sicherheits- und Speicherungslösungen verschaffen Administratoren ein Instrumentarium zur Erstellung von Regeldefinitionen und zur Codierung von Ereigniskorrelations- und Automatisierungsinformationen.

IBM hat fünf Implementierungsstufen für selbstschützende IT-Infrastrukturen definiert:

Basic Stufe 1	Managed Stufe 2	Predictive Stufe 3	Adaptive Stufe 4	Autonomic Stufe 5
Definition • Sicherheitskontrollen werden in jedem Gerät separat installiert (in unterschiedlichen Formaten) • IT-Sachwerte des Unternehmens werden durch einfache Infrastrukturtools geschützt.	**Definition** • Sicherheits-konfigurationen für Geräte werden zentral verwaltet. • In der gesamten Infrastruktur sind Intrusionssensoren vorhanden	**Definition** • Verwaltung der Anwendungssicherh eit nach einheitlichen Sicherheitsregeln • Korrelation von Intrusionsereignissen zur Unterscheidung wirklicher Angriffe von Routineabläufen • Konsolidierte Anmeldung	**Definition** • Sicherheitsrelevante Zugriffe werden nach Regeln gestattet; dynamische Anpas-sung des Zugriffs an Regeländerungen. • Konfiguration von Intrusions-Erken-nungstools passt sich an IT-Sicherheits-regeln und Gefährdungs-situationen an.	**Definition** • Kontext der e-business-Sicherheit • Selbständig kooperierende Systeme zur Erkennung von Angriffen, Verifizierung und Umkonfiguration • Erlernte Regeln zum zukünftigen Schutz
Vorteile Verringerung der Ausgaben im IT-Bereich	**Vorteile** Verbesserter Schutz der IT-Sachwerte	**Vorteile** Verbesserte Anwendungssicherheit mit einheitlicher Sicherheitsinfras-truktur	**Vorteile** Sicherheitsinfrastruktu r reagiert selbständig unter minimalem menschlichem Eingreifen	**Vorteile** Bindung der Peripherie- und Anwendungssicherheit an Geschäftsregeln

Stufe 1: Basic
Die Sicherheitskonfiguration auf lokaler Basis erfordert die separate Konfiguration jeder Komponente sowie die manuelle Nachverfolgung von Veränderungen. Zur Datensicherung werden lokale Sicherungs- und Wiederherstellungstools eingesetzt. Prüfprotokolle werden für jeden Rechner separat erstellt. Der Schutz des Systems während der Laufzeit und der Schutz der Geschäftsdaten erfordern ständiges menschliches Eingreifen.

Stufe 2: Managed
Die Sicherheitsadministration ist durch den Einsatz von Management-Tools zentralisiert; Benutzer-IDs können zentral erstellt, Zugangsrechte zu Ressourcen können zentral verwaltet werden. Zur Erkennung von Eindringversuchen werden Intrusionsdetektoren und Prüfprotokoll-Tools verwendet. Diese werden manuell ausgewertet, und entsprechende Maßnahmen zum Schutz gegen zukünftige Angriffe werden von Mitarbeitern ergriffen. Zentrale Datens-icherungs- und -wiederherstellungstools wirken ressourcenübergreifend.

Stufe 3: Predictive
Mit unternehmensweiten Security-Management-Tools können Sicherheitsregeln manuell und konsistent umgesetzt werden. IDs und Zugangsrechte werden anwendungsübergreifend koordiniert und können nötigenfalls konsistent

widerrufen werden. Sensoren im Peripheriebereich können Sicherheitsverletzungen erkennen und echte Angriffe durch Korrelation identifizieren. Security-Tools empfehlen Korrekturmaßnahmen.

Stufe 4: Adaptive
Das Security-Management nutzt hochentwickelte Automatisierungstechnologie; so können neue Nutzer automatisch registriert und IDs von ausgeschiedenen Nutzern deaktiviert werden. Das System gewährt automatisch Zugang zu Systemen und Anwendungen, die zur Erledigung einer neuen Aufgabe gebraucht werden, und verwehrt den Zugang zu Systemen, die für vorhergehende Aufgaben benötigt wurden. Werden unberechtigte Zugriffs- und Eindringversuche erkannt, werden automatisch Umkonfigurationsmaßnahmen eingeleitet, um Teilsysteme zu isolieren und den Zugang zu IDs zu blockieren.

Stufe 5: Autonomic
Die Betonung liegt auf der Lernfähigkeit von Systemen sowie auf Systemen, die untergeordnete Ressourcenmanagement-Regeln an übergeordneten Geschäftsregeln ausrichten. Da die Systemkomponenten miteinander kooperieren, können Systeme im laufenden Betrieb umkonfiguriert werden; Security-Patches können im Bedarfsfall automatisch installiert werden; die Intensität der Intrusionsüberwachung kann an die geschäftlichen Erfordernisse angepasst werden; und Regeln können auf der Grundlage gemachter Erfahrungen verändert werden, um zukünftige Probleme zu verhindern.

Systemschutz durch Tivoli Softwareprodukte

Folgende Tivoli Softwareprodukte eignen sich zur Implementierung einer selbstschützenden Umgebung:

IBM Tivoli Storage Manager
IBM Tivoli Storage Manager gewährt autonomen Schutz durch automatische Sicherung und Archivierung von Unternehmensdaten über heterogene Speicherumgebungen hinweg. Sein Schutz kann auf Tausende von Rechnern mit einem Dutzend verschiedener Betriebssysteme ausgedehnt werden. Die intelligenten Datenverlagerungs- und Datenspeicherungsverfahren sowie umfassende Automatisierungsfunktionen reduzieren die Administrationskosten und steigern die Dienstqualität.

IBM Tivoli Access Manager
Die Lösungen der Produktfamilie IBM Tivoli Access Manager sind selbstschützend, da sie unerlaubten Zugriff verhindern und über einen einzigen Security-Policy-Server Sicherheitsregeln auf unterschiedliche Dateitypen, Anwendungen, Geräte, Betriebssysteme und Protokolle anwenden. Sie unterstützen viele verschiedene Benutzerauthentifizierungsverfahren einschließlich der konsolidierten Anmeldung per Internet und der Steuerung des Zugangs zu vielen verschiedenen Arten von Ressourcen mit Benutzerauthentifizierung.

Tivoli Identity Manager
IBM Tivoli Identity Manager realisiert das Konzept des Selbstschutzes durch zentralisiertes Identitätsmanagement, durch die Kopplung automatischer Workflows mit Geschäftsprozessen und die Nutzung produktivitätssteigernder Selbstbedienungs-Benutzeroberflächen.

Tivoli Risk Manager
IBM Tivoli Risk Manager sorgt für systemweiten Selbstschutz durch Auswerten möglicher Sicherheitsbedrohungen und automatisches Einleiten von Gegenmaßnahmen, z.B. durch Server-Umkonfiguration, Implementierung von Security-Patches und Zwangsschließung von Zugangskonten. Es erfasst Sicherheitsinformationen von Firewalls, Intrusionsdetektoren, Vulnerability-Scannern und anderen Security-Instanzen. Es vereinfacht und korreliert die Vielzahl der Ereignismeldungen und Warnungen, die von den zahlreichen Sicherheitsinstanzen generiert werden, und identifiziert rasch die tatsächlichen Sicherheitsbedrohungen, so dass Administratoren mit angemessenen Gegenmaßnahmen reagieren können.

IBM Tivoli Privacy Manager for e-business
IBM Tivoli Privacy Manager for e-business wirkt selbstschützend, indem es viele mit der Security-Compliance verbundene Vorgänge automatisiert und die Kopplung von Vertraulichkeitsregeln mit Geschäftsprozessen sowie ihre Überwachung und Umsetzung vereinfacht. Es registriert die Regelzustimmung bzw. -ablehnung durch Endanwender, kann die Einhaltung von Zugangsregeln überwachen und durchsetzen und Prüfprotokollberichte erstellen.

Fazit

Companies want and need to reduce their IT costs, simplify management of their IT resources, realize a fast return on their IT investment and provide high levels of availability, performance, security and asset utilization. Autonomic computing helps address these issues. IBM is a leader in the evolution to autonomic computing and offers integrated systems management solutions for resource management, transaction-oriented management and business-solution management that span the four autonomic computing disciplines of self-configuring, self-healing, self-optimizing and self-protecting.

Weitere Informationen

Informationen zu Tivoli Software und integrierten Lösungen von IBM erhalten Sie von Ihrem IBM Vertriebsbeauftragten oder im Internet unter:
ibm.com/tivoli

IBM Deutschland GmbH
70548 Stuttgart
http://www.**ibm.com**/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
http://www.**ibm.com**/at

IBM Schweiz
Bändliweg 21, Postfach
8010 Zürich
http://www.**ibm.com**/ch

10-02

Die Tivoli Homepage finden Sie im Internet unter
ibm.com/tivoli

Die IBM Homepage finden Sie im Internet unter
ibm.com

e business software