

## Nutzen und Motivation für Discovery Systeme

**Situation:** Discoverwerkzeuge und hier insbesondere Application Discovery Tools erfahren zur Zeit nicht nur aufgrund der notwendigen Ermittlung von Basisdaten für ein Business Service Management ein großes Interesse. Auch für die Konsolidierung verschiedener IT-Landschaften oder Rechenzentren werden aktuelle verlässliche Informationen benötigt, bei deren Beschaffung ein Discoverywerkzeug helfen kann.

- *Configuration Management Data Base (CMDB)*
- *Discovery der gesamten IT-Infrastruktur*
- *Automatisierte Erfassung der Applikationen und Abhängigkeiten zur Infrastruktur*
- *Business Service Management*
- *Serverkonsolidierung*

### Motivation

- *Aktuelle Informationen über den IST-Zustand der IT-Infrastruktur*
- *Befüllung u. Verifikation einer CMDB*
- *Fehlerbehebung (Minimierung von Ausfallzeiten)*
- *Erfüllung von Richtlinien (Basel II, SOX, ...)*
- *Lizenzmanagement*
- *Ressourcenoptimierung (Verbesserung der Kapazitätsauslastung)*
- *EAM (Strategie- und Migrationsplanung)*
- *Change Monitoring*
- *Outsourcing (Umgebung nachbauen)*
- *Compliance Check*
- *Changeverifikation*
- *Datengrundlage für Prozessmonitoring*

**Spricht** man von Scanwerkzeugen, reicht das Spektrum der zu betrachtenden Werkzeuge von einfachen Barcode-scannern bis hin zu Application Discovery Systemen. Für verschiedene Zielsetzungen kommen unterschiedliche Scanwerkzeuge zum Einsatz. Für die Standortbestimmung der Geräte, den Wareneingang und die Auftragsverfolgung (Umzug, Abbau, Aufbau) werden manuelle Scanwerkzeuge verwendet, die mit Hilfe von Barcodescannern den aktuellen Standort, das Produkt, Inventar- und Seriennummer erfassen können und an die CMDB liefern. Weiterhin sind automatisierte Scanwerkzeuge erhältlich bei denen man unterscheidet zwischen

Inventoryscannern und Applikation Discovery Systemen. Inventoryscanner sind spezialisiert auf die automatische Erfassung von Hard- und Software der unterschiedlichen Systeme. Diese gibt es in verschiedenen Ausprägungen und Fähigkeiten, unterschiedliche Systeme zu scannen (Windows- Unix Server, Switches, Router, Firewalls, ...). Systeme zur Softwareverteilung beherrschen diese Disziplin meist auch, da diese auf die Daten angewiesen sind.

Application Discovery Systeme haben die besondere Fähigkeit, auf den Systemen laufende Applikationen (Prozesse) zu erkennen und die Abhängigkeiten zu verschiedenen Servern und anderen Prozessen zu ermitteln. Beispiel hierfür wären die Abhängigkeit einer Web Applikation zum Server und der Datenbank, die auch auf einem anderen Server laufen kann. Dies noch eine relativ neue Disziplin (im Vergleich zu den Inventorywerkzeugen) aber aufgrund der fortschreitenden Serviceorientierung der IT Abteilungen nach ITIL sehr wichtig. Auch im Rahmen eines BSM (Business Service Management) Projektes zur Überwachung der Services, die an die Kunden verkauft werden, ist dies ein wichtiges Element, da meistens gar nicht exakt bekannt ist, welche Abhängigkeiten bestehen und die Scanner diese entweder direkt liefern oder zumindest Änderungen aufzeigen können. Manch einer hat schon eine Überraschung erlebt, welche bislang unbekanntes Abhängigkeiten die Systeme liefern, obwohl man der Meinung war diese für einzelne Applikation genau aufzeigen zu können. Ein Application Discovery kann also helfen, die Service Bäume ab einer Ebene, die automatisiert ermittelbar ist, zu ergänzen oder aktuell zu halten.

## Agentenbasierte Verfahren

**Die** Discovery Systeme lassen sich technisch in drei Gruppen aufteilen: agentenbasiert, agentenlos und passiv.

**Agentenbasierte** Systeme arbeiten über eine Software (einen Agenten), der zunächst auf den Zielsystemem installiert werden muss. Diese ermitteln die Konfigurationsinformationen und senden diese zeit- oder ereignisgesteuert an den zentralen Manager (Pushverfahren). Dies hat eine relativ niedrige Netzlast zur Folge, da hier meist nur Deltadaten gesendet werden. Andererseits kann der zentrale Manager die Agenten zeitgesteuert abfragen, wodurch auch Ausfälle der Agenten erkannt werden.

Das agentenbasierte Verfahren hat verschiedene **Vorteile**: die operationelle Kontrolle ist besser, da die Agenten einfacher überwacht werden können (trace, debug) und auf die entsprechenden Betriebssysteme besser angepasst sind. Die Agenten bieten mehr Funktionalität und ermöglichen z.B. erst ein realtime Monitoring also eine Lieferung von Konfigurationdaten direkt nach deren Änderung. Durch die lokale Datensammlung hat man keinen Verlust der Daten bei Übertragungsfehlern und die Datensammlung ist vom eigentlichen Scanlauf getrennt. Der Scan vieler Systeme erfolgt hier schneller, da die Agenten losgelöst vom zentralen Manager nur mit den lokalen Ressourcen arbeiten. So können prinzipiell alle Systeme gleichzeitig gescannt werden. Ein wichtiger Vorteil wäre noch die Möglichkeit die Systeme von Außendienstmitarbeitern und Heimarbeitsplätzen zuverlässig scannen zu können, da die Daten auf den Systemen ermittelt werden und zum Zeitpunkt der Onlineverbindung von den Agenten aktiv gesendet werden.

**Nachteile** der agentenbasierten Lösung: Der Agent muss zunächst auf jedem System installiert werden, wodurch evtl. eine Softwareverteilung benötigt wird. Die Agenten benötigen auf den jeweiligen Systemen auch wieder Ressourcen und verursachen höhere administrative Aufwände, da diese z.B. bei neuen Versionen aktualisiert werden müssen. Durch unterschiedliche Lizenzierungsmodelle für verschiedene Plattformen, können höhere Kosten entstehen.

### Mehrwert

*Ein Discovery bietet Mehrwert für unterschiedliche Gruppen:*

#### • Unternehmen

- bei größeren Unternehmen mehr als kleinen (aufgrund der Investitionskosten)
- IT-Service Dienstleister
- Service Provider
- Unternehmen mit vielen Komponenten, die in hohem Maße voneinander abhängig sind und ein durchgängiger Betrieb notwendig ist

#### • Anwender

- Minimierung von Ausfallzeiten
- Übersicht über die Applikationslandschaft, die bisher nicht zu beschreiben war (jeder wusste nur etwas)

#### • Netzwerk Administratoren

- Verbesserung der Kapazitätsplanung
- Soll-Ist Vergleich (Compliance Check)
- Impactanalysen (Auswirkungen auf Geschäftsprozesse)
- Dadurch Bewertung der Dringlichkeit einer Störung

## Agentenlose und passive Verfahren

**Bei den agentenlosen Verfahren** wird keine zusätzliche Software auf den Zielsystemen installiert, sondern während des Scanvorganges sogenannte Sensoren (kleine Programme, meist Scripte) temporär übertragen und nach dem Scanvorgang wieder gelöscht. Der Scan erfolgt per SNMP, ssh, WMI, JMX oder Port Scans. Üblicherweise werden keine Daten lokal gespeichert.

**Vorteile** dieser Lösung sind: Stark reduzierte Implementierungsaufwände und einfache Handhabung. Einfaches Deployment, da diese Systeme teilweise fertig konfiguriert geliefert werden oder nur ein System installiert werden muss. Meist werden auch geringere Ressourcen auf den Zielsystemen genutzt.

**Nachteile** dieser Lösung sind: Datenverlust bei Störungen und eine temporär höhere Last im Netzwerk. Der gesamte Prozess wird zentral von einem Punkt gesteuert, wodurch mehr kritische Fehlerpunkte zu beachten sind. Ein realtime Scan ist kaum möglich, da nur eine begrenzte Anzahl System gleichzeitig bearbeitet werden können. Der wichtigste Punkt ist jedoch, dass die Systeme nur vernünftige Daten liefern können, wenn eine Anmeldung auf den Systemen erfolgen kann. Es müssen also credentials (Logininformationen) für alle Systeme gepflegt werden. Weiterhin ist ein Scan von Aussendienstmitarbeitern und Heimarbeitsplätzen fast nicht möglich, da bei diesem Verfahren nur Geräte gefunden werden, die zum Zeitpunkt und während des gesamten Zeitraums des Scans online sind.

### Beispiele für agentenbasierte Inventory Systeme

- BMC Configuration Discovery
- CA Desktop Management
- Enteo NetInstall
- LANDesk Managementsuite
- Matrix42
- Microsoft SMS
- Novell ZAM (ehem. TS.Census)
- Symantec Altiris
- Tivoli Inventory

### Agentenlose Systeme

- BDNA Insight
- BMC Foundation Discovery
- xAssets Network Discovery

### Beispiele für Application Discovery systeme

- BMC Topology Discovery
- CA Dependancy Mapping (ehem. Cohesion)
- EMC<sup>2</sup> ADM (ehem. nLayers)
- Tideway Foundation
- HP DDM
- IBM TADDM
- mValent Integrity (demnächst Oracle))
- Symantec Veritas Configuration Manager

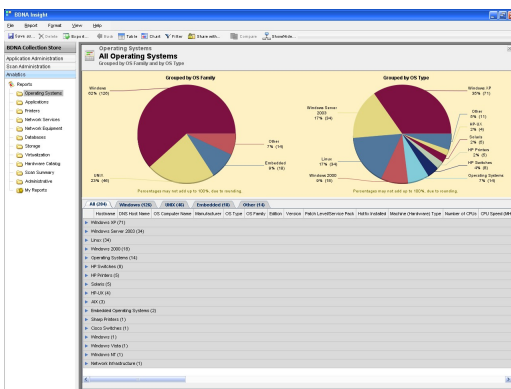
**Beim passiven Discovery** wird rein passiv der Netzverkehr analysiert (wer spricht mit wem, genutzte Protokolle, Datenrate). Durch Kenntnis der Transaktionen der Applikationen können so Rückschlüsse über die aktiven Services und Ihre Abhängigkeiten ermittelt werden.

**Vorteilhaft** ist die einfache Installation (Appliance). Auf den Zielsystemen werden keinerlei Ressourcen benötigt und es wird auch keine zusätzliche Netzlast erzeugt. Es kann durchgängig gescannt werden, wodurch man Echtzeitinformationen erhält und auch Kommunikationswege mitbekommt, die nur temporär bestehen. Durch Messung der Anzahl und der Datenrate zwischen zwei Teilnehmer kann man zusätzlich eine gewisse Priorisierung ermitteln, wobei die Datenrate nicht unbedingt Auskunft über die Relevanz der Kommunikation für die Geschäftsprozesse gibt.

**Nachteilig** wirkt sich hingegen die begrenzte Netzabdeckung aus, da nur die Kommunikation innerhalb des lokalen Netzes und auch nur die, die über den Switch läuft, an den das System angeschlossen ist, analysiert werden kann. Mit diesem Verfahren können auch keine Konfigurationsinformationen der CIs ermittelt werden, was dazu führt, dass dieses Verfahren meist nur in Kombination mit einer der anderen oben genannten Verfahren verwendet wird.

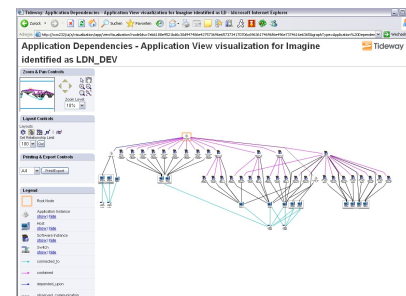
## Application Discovery Systeme unterstützen den Betrieb

**Alle** aufgeführten Application Discovery Systeme arbeiten agentenlos und sind deswegen gut geeignet, um schnell zu einem Ergebnis zu kommen. Einige der Systeme werden als Appliance geliefert, wodurch man Installations- und Konfigurationsaufwände spart. Einige Anbieter, wie z.B. BDNA und Tideway bieten daher auch Mietlizenzen oder auch Kurzinstallationen an, wo ein System für einige Tage das Netzwerk scannt und man die Daten anschließend weiterverwenden darf. Dies bietet sich an, wenn für ein Projekt bestimmte Daten benötigt werden, die aktuell nicht zur Verfügung stehen und nach Ende des Projektes auch nicht unbedingt weiter benötigt oder dann manuell gepflegt werden.



**Alle Lösungen** haben Ihre Vor- und Nachteile. Sie unterscheiden sich z.B. in den unterstützten Systemplattformen und scanbaren Plattformen (Mainframe, Server OS, Switch OS, ..) oder der Erweiterbarkeit für eigene Applikationen (Custom Scans). Einige werden vom Hersteller innerhalb einer Suite angeboten oder bieten gute Integrationsmöglichkeiten. Eine Auswahl eines Systems sollte daher auf Basis eines gewichteten Kriterienkataloges erfolgen. Es ist auch nicht ungewöhnlich, wenn mehrere Systeme (auch unterschiedlicher Hersteller)

für unterschiedliche Plattformen (Client / Server) parallel eingesetzt werden. Ein Betrieb einer Discoverylösung als Inselsystem macht jedoch meist keinen Sinn. Die Integration in eine CMDB und damit in die Serviceprozesse ist daher eine der wichtigsten Aktivitäten. Aus diesem Grund liefern die Werkzeuge meist auch schon eine Standardintegration in eine oder sogar mehrere CMDB'en mit.



Unter [www.comconsult.de](http://www.comconsult.de) finden Sie weiterführende Informationen und Projektbeispiele. Als Garant für den Projekterfolg stehen unsere langjährige Erfahrung und Fachkompetenz bei allen aktuellen Themen, genaue Marktkenntnisse, detailliertes Produktknowhow und leistungsfähige Kopplungen zu den bekanntesten Produkten für das Service-, Netzwerk- und Systemmanagement.

### Profitieren auch Sie von unserer Erfahrung!

Sie erhalten von uns eine kompetente und herstellernerneutrale Projektunterstützung in allen aktuellen Bereichen des IT-Infrastructure- und Change-Managements. Wir helfen Ihnen bei der Auswahl und Implementierung von geeigneten Zusatzwerkzeugen genauso wie bei der Entwicklung, Kopplung und Integration von Speziallösungen. Unser umfangreiches Repertoire an Optimierungsmöglichkeiten umfasst die Automatisierung Ihres Tagesgeschäfts, die Sicherung Ihrer Datenbestände und die konsistente Zusammenführung vorhandener Daten- und Funktionspools unter dem Dach einer zentralen CMDB. Mit uns erhalten Sie **einen Ansprechpartner für alles**, der Ihre speziellen Wünsche durch geschicktes Customizing und zuverlässige, standardbasierte Individuallösungen erfüllt. Rufen Sie uns an – wir beraten Sie gerne.

**Ihr Ansprechpartner:**

Guido Parletta, Abteilungsleiter (Guido.Parletta@comconsult.de)

Disclaimer: Dieses Informationsmaterial beinhaltet keine Garantiezusagen, verbindliche Vertragsangebote oder Vorgaben für spätere Vertragsinhalte. Der jeweilige Vertragsinhalt wird gesondert mit unseren Kunden nach den Gegebenheiten des Einzelfalles vertraglich festgelegt.