IBM Tivoli Application Dependency Discovery Manager (TADDM 4.1)

Technische Architektur – Übersicht

1. Kurzübersicht

Die heutigen IT-Unternehmen stehen unter einem enormen Druck, wenn es darum geht, Services von hoher Qualität flexibel und effizient bereitzustellen. Gleichzeitig können sie häufig nur reagieren statt zu agieren. Dabei müssen sie immer noch auf ungeeignete Tools und manuelle Prozesse zurückgreifen, um Probleme in Umgebungen zu lösen, die zunehmend komplexer werden und ständigen Veränderungen unterliegen. Die durch Komponentenarchitekturen wie J2EE und .NET bewirkte Komplexität führte zu deutlich mehr Virtualisierung auf Software-, Betriebssystem- und Netzwerkebene. Darüber hinaus machten die gestiegenen geschäftlichen Anforderungen ein gemeinsames Verständnis der Konfiguration und der Beziehungen der einzelnen IT-Infrastrukturkomponenten untereinander erforderlich. Dies war gerade bei der Bereitstellung von Geschäftsanwendungen und letztendlich für den Erfolg im IT-Bereich von ausschlaggebender Bedeutung[1]. Führende IT-Unternehmen sind zur Zeit dabei, Lösungen für diese Problematik zu bewerten und zu implementieren, wobei Produkte zur Erstellung von Anwendungsübersichten wie IBM Tivoli Application Dependency Discovery Manager (TADDM) zum Einsatz kommen. Diese Lösungen ermöglichen ein gemeinsames Verständnis der Komponenten, Abhängigkeiten und Konfigurationen kritischer Geschäftsanwendungen. Diese Transparenz ist gerade hinsichtlich der Einhaltung von SLAs (Servicel-Level-Agreements), der Vermeidung von Problemen durch unerwartete Veränderungen oder der Verkürzung von Problembehebungszeiten von besonderer Bedeutung. Und sie spielt auch bei der Umsetzung technologischer Konsistenz, der Realisierung von Prozesskonformitäten und Compliancerichtlinien sowie der Implementierung flexibler und schneller Veränderungen eine gewichtige Rolle.

Damit die erforderlichen Transparenzebenen auch erreicht werden können, muss eine Lösung folgende Kriterien erfüllen:

- Bereitstellung einer vollständig automatisierten und detailgenauen Sicht in der Laufzeitstruktur von Geschäftsanwendungen, wobei die Anwendung selbst im Mittelpunkt stehen muss. Dies umfasst alle Software- und Hardwarekomponenten der Anwendung sowie die schichtübergreifenden Abhängigkeiten und Konfigurationen[1].
- Speicherung der Anwendungsübersichten und der zugehörigen Daten in einer gut strukturierten und definierten Datenbank für Anwendungsübersichten, die sich durch folgende Merkmale auszeichnet:
    - Großes Speichervermögen, damit alle gemeinsamen Rechenzentrumskomponenten zur Laufzeit abgedeckt sind, und gleichzeitig hohe Flexibilität, um den jeweiligen Anforderungen der einzelnen Implementierungen gerecht zu werden

[1] Siehe Gartner (Colville) „Organizations Are Paying More Attention to Configuration Management“ 31. März 2005 und Enterprise Management Associates „The ITIL Configuration Management Database: Panacea or Pandora’s Box?“ Dezember 2004.

    - Detailgenauigkeit, um fundierte Konfigurations- und Abhängigkeitsdaten zur Laufzeit bereitzustellen
    - Einfache Zugriffsmöglichkeiten und hohe Benutzerfreundlichkeit für das Betriebspersonal
    - Gemeinsame Nutzung mit anderen Management- und Unternehmensanwendungen
- Skalierbarkeit bis zur Unternehmensebene
- Schnelle, sichere und effiziente Wertschöpfung
- Sichere Implementierung und Nutzung unter Beachtung der geltenden Sicherheitsrichtlinien und Infrastrukturen im Unternehmen

Und dies sind genau die hohen Produktanforderungen, die letztendlich das Design und die Architektur des führenden IBM Produkts zur Erstellung von Anwendungsübersichten IBM Tivoli Application Dependency Discovery Manager (TADDM) bestimmten. Um diesen Anforderungen gerecht zu werden, wurden fünf kritische Designentscheidungen in der Architektur von TADDM umgesetzt:

1) Aufbau des Produkts um ein vordefiniertes, anwendungsorientiertes Referenzmodell, das auf Standards basiert und erweiterbar ist. So entfällt die Notwendigkeit, das Modell bei jeder Implementierung neu anpassen zu müssen.
2) Berücksichtigung eines agentenfreien Lösungsansatzes, um Leistungs- und Sicherheitsrisiken sowie Implementierungs- und Qualifizierungskosten für die Implementierung neuer Managementagenten zu vermeiden.
3) Veröffentlichung eines durchdachten Schemas mit umfassenden Dokumentationsdaten und Prozess-APIs, wodurch eine schnelle Integration in vorhandene Managementprodukte und -prozesse ermöglicht wird.
4) Möglichkeiten zur Einbindung und Erweiterung der Datenbank für Anwendungsübersichten, wodurch das Produkt auf Unternehmensebene implementiert werden kann.
5) Verwendung vorhandener sicherer Protokolle und Standards, wodurch eine sichere und unkomplizierte Implementierung erfolgen kann.

Die kombinierte Umsetzung dieser zentralen Designentscheidungen resultiert in einer Lösung, die umfassend und transparent aufzeigt, wie die Infrastruktur Anwendungen und Services bereitstellt, schnell und sicher implementiert bzw. wie sie auf einfache Weise integriert, skaliert und erweitert werden kann. Darüber hinaus lässt sich mit einer solchen Lösung darstellen, wo die Gesamtbetriebskosten am niedrigsten sind. Bei Lösungen, die solche Bereiche nicht abdecken, treten sehr schnell Probleme in Bezug auf Zeit und Kosten auf, wenn es darum geht, die Transparenzebene bereitzustellen, die für das Management und die Verbesserung der Servicebereitstellung erforderlich ist.

Dieses White Paper bietet technischen Entscheidern eine detaillierte Beschreibung der TADDM-Architektur und geht darauf ein, wie das Produkt eine Infrastruktur vollständig und transparent darstellen kann. Im Einzelnen sind folgende Informationen enthalten:

- Überblick über die TADDM-Architektur
- Ausführliche Beschreibung zur Erstellung und Verwaltung von Anwendungsübersichten durch TADDM

- Erläuterung der TADDM-APIs und Integrationsfunktionen
- Überblick über die TADDM-Implementierungsarchitektur
- Überblick über die Funktionen für Sicherheit, Skalierbarkeit und Zuverlässigkeit

Mit IBM TADDM verbessern Unternehmen nicht nur die Anwendungsverfügbarkeit und senken ihre Kosten, sondern bilden damit die Grundlage für den Aufbau einer echten IT-Service-Management-Umgebung mit umfassendem Funktionsspektrum und hoher Skalierbarkeit. Die mit Hilfe von TADDM erstellten Daten und das daraus resultierende Wissen bilden einen zentralen Baustein nicht nur zur Verbesserung von Servicebereitstellung und -management, sondern auch in Bezug auf die Automatisierung und Nutzung von Funktionen wie die dynamische Anwendungsbereitstellung, messbare und umsetzbare SLAs (Service-Level-Agreements) sowie effiziente IT-Governance. Letztendlich geht der Autor dieses White Papers auch auf die Architektur und die Features von TADDM ein, um diese Funktionalität bereitstellen zu können.

2. Die Architektur im Überblick

Die agentenfreie, modellorientierte Architektur von TADDM ist in Abbildung 1 dargestellt. Dieser Abschnitt enthält eine Kurzbeschreibung zu jedem Element. Abschnitt 2 enthält Einzelheiten zu den wichtigsten Architekturkomponenten. Zum einen werden dabei die Gründe für das jeweilige Design und ein Überblick über dessen Implementierung aufgeführt, zum anderen wird erläutert, wie die einzelnen Komponenten zusammenwirken, um die Datenbank für Anwendungsübersichten mit Daten zu füllen und die Anwendungsübersichten zu erstellen und zu verwalten.

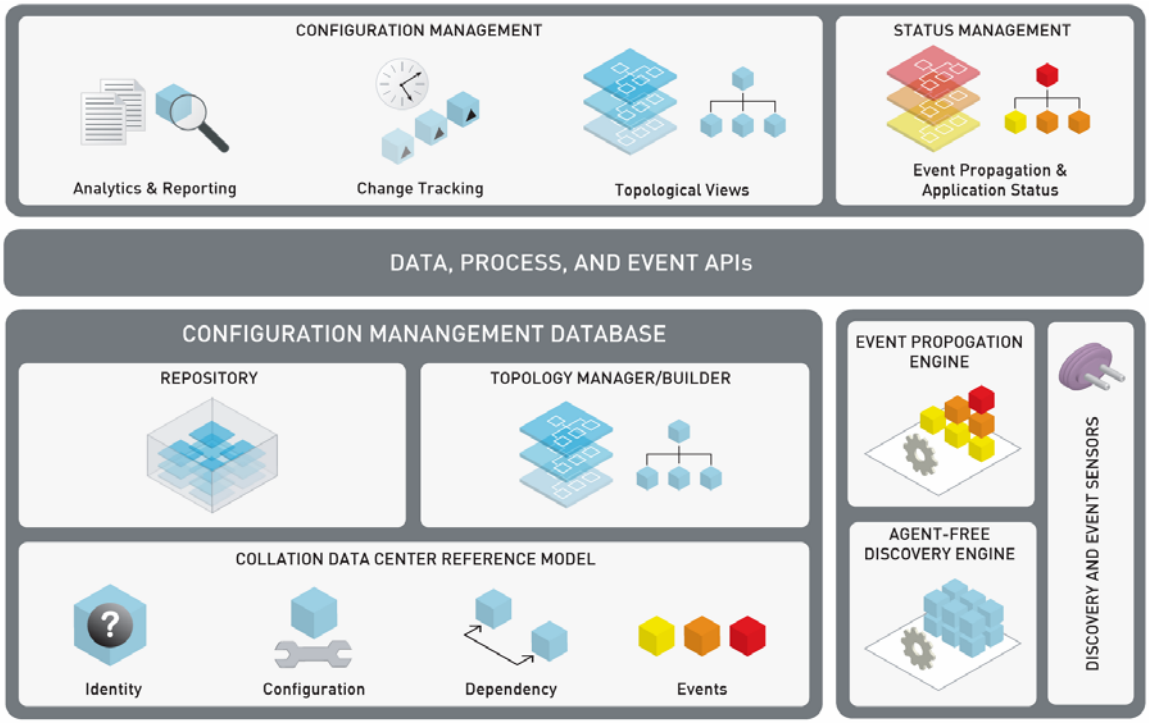


Abb. 1: Die TADDM-Serverarchitektur

IBM Data Center Reference Model: Dieses Modell ist die Basis von TADDM und umfasst die Definition für die Anwendungen im Rechenzentrum, die unterstützenden Infrastrukturkomponenten, die schichtübergreifenden Beziehungen und die Konfigurationsattribute. Ohne ein solches Referenzmodell hinge die Implementierung von einem kostspieligen, zeitaufwendigen manuellen Modellierungsansatz ab, der zudem unvollständig und fehlerbehaftet wäre. TADDM hingegen zeichnet sich durch sofort einsatzfähige Definitionen für eine Vielzahl gängiger Softwareanwendungen, Hosts, Netzwerkeinheiten und -services aus. Das erweiterbare Referenzmodell umfasst zudem ein Ereignisweitergabemodell (Event Propagation Model), das die Grundlage für die Interpretation von Infrastrukturkomponentenereignissen im Kontext der Anwendungen bildet, die sie bereitstellen.

Agent-Free Discovery Engine: Die Discovery-Engine koordiniert und verwaltet den gesamten Erkennungsprozess. Dabei instruiert die Engine die „Erkennungssensoren“ (Discovery Sensors), bei denen es sich um serverbasierte Komponenten handelt, die das im Referenzmodell enthaltene Wissen nutzen, um die Komponenten im Rechenzentrum abzufragen und die für den Aufbau der Datenbank für Anwendungsübersichten erforderlichen Informationen zusammenzustellen.

Topology Manager/Builder: Nach Abschluss des Erkennungsprozesses konsolidiert der Topology Manager die ermittelten Daten und generiert eine schichtübergreifende topologische Darstellung der Anwendung. Diese Anwendungstopologie umfasst alle zu Grunde liegenden Infrastrukturkomponenten (Software, Systeme und Netzwerkkomponenten) sowie die jeweiligen Konfigurationen und schichtübergreifenden Abhängigkeiten.

TADDM Application Map Database: Die TADDM-Datenbank ist eine schichtübergreifende Darstellung der Anwendungstopologie, ihrer Komponenten und deren Konfigurationen. Die Datenbank verfolgt und dokumentiert zudem alle Konfigurationsänderungen. Die TADDM-Datenbank ermöglicht sowohl Lese- als auch Schreibzugriff und bietet umfangreiche Abfragemöglichkeiten.

TADDM API: Die offene und veröffentlichte API von TADDM harmoniert problemlos mit Anwendungen anderer Anbieter aus dem direkten Geschäftsumfeld. Die TADDM-API bietet authentifizierten und sicheren Zugriff auf die zu Grunde liegende TADDM-Datenbank (über die Daten-API) und die TADDM-Prozessengines (über die Steuerungs-API). TADDM enthält darüber hinaus eine Ereignis-API, über die Ereignisse in andere/aus anderen Managementanwendungen importiert/exportiert werden können.

TADDM User Interface: Durch den Zugriff auf die TADDM-Datenbank und die TADDM-Discovery-Engine über die TADDM-APIs bietet die TADDM-Benutzerschnittstelle Befehle und Steuerungsmöglichkeiten für den TADDM-Server, erweiterte Topologievisualisierung und -management sowie leistungsfähige Funktionen für Änderungs- und Konfigurationsanalyse.

TADDM Application Status Manager: Der Application Status Manager nutzt das auf der TADDM-Topologie basierende Ereignisweitergabemodell (Event Propagation Model) und importiert komponentenbasierte Ereignisse aus Überwachungslösungen über TADDM-Ereignissensoren. Solche Ereignisse werden im Rahmen der jeweiligen Geschäftsanwendungen weitergegeben. Dadurch wirken sich Ereignisse auf Komponentenebene nahezu unmittelbar auf den Anwendungsstatus aus.

3. Die Architektur im Detail

3.1 Das IBM Data Center Reference Model

Das TADDM Data Center Reference Model stellt eine Definition der Infrastrukturkomponenten im Rechenzentrum, der schichtübergreifenden Beziehungen und der Konfigurationsattribute dar. Dieses Modell basiert auf dem CIM 2-Objektmodell von DMTF[2] mit plattformspezifischen Erweiterungen wie JSR 77[3]. Das Referenzmodell umfasst eine Vielzahl unterschiedlicher Objekttypen einschließlich verschiedener Softwarekomponenten (Web, Anwendungen, DB-Server), Hosts und Betriebssysteme, Netzwerkelemente (Router, Switches, Load Balancer, Firewalls, Speicherkomponenten) und Netzwerkservices (LDAP, NFS, DNS). Das Modell kann problemlos je nach Kundenanforderungen erweitert werden.

Die Modelldarstellung für jeden Komponententyp umfasst Folgendes:

- *Signatur:* Die Signatur identifiziert eindeutig den Komponententyp und dessen Abhängigkeits- und Konfigurationsschablone.
- *Konfigurationen:* Konfigurationsdatenelemente umfassen die statischen und dynamischen Konfigurationen der Komponente, die von der Komponente verwendeten Laufzeitressourcen (z. B. die JDBC-Verbindungspools oder die von einem Anwendungsserver verwendete JMS-Themenwarteschlange, die Programmkorrekturen (Patches) für ein Betriebssystem oder die IP-Routetabelle eines Netzwerkelements) sowie die implementierten Anwendungsobjekte (z. B. die EJBs und JSPs auf einem Anwendungsserver), durch die die Geschäftsanwendung und die Services implementiert werden.
- *Abhängigkeiten:* Abhängigkeiten modellieren die Beziehungen zwischen den verschiedenen Komponenten innerhalb des Rechenzentrums. TADDM ermittelt verschiedene Typen schichtübergreifender Abhängigkeiten und kategorisiert diese wie folgt:
    - *Transaktionale Abhängigkeiten:* Die logischen (IP-basierten) Verbindungen zwischen den Komponenten einer verteilten Anwendung. Diese Verbindungen geben die Anbieter-Verbraucher-Beziehungen zwischen den Komponenten an. Ein Anwendungsserver ist beispielsweise der Verbraucher eines von einem Datenbankserver bereitgestellten Service.
    - *Einschlussabhängigkeiten:* Schichtübergreifende hierarchische Beziehungen (z. B. ein auf einem Host implementierter Anwendungsserver) sowie logische Gruppenbeziehungen (z. B. ein Web-, ein Anwendungs- und ein Datenbankserver bilden eine Geschäftsanwendung).
    - *Serviceabhängigkeiten:* Netzwerkservices, von denen die meisten Infrastrukturkomponenten abhängen (NFS-, DNS- und LDAP-Services).

---

[2] Siehe www.dmtf.org

[3] Siehe http://www.jcp.org/en/jsr/detail?id=77

3.2 Agent-Free Discovery Engine und der dahinterstehende Prozess

Die agentenfreie Discovery-Engine von TADDM verwaltet den gesamten Erkennungsprozess. Bei diesem Prozess werden die Daten erfasst, die für die Instanziierung des Data Center Reference Model benötigt werden, um die spezielle Rechenzentrumsinfrastruktur darzustellen. Kernpunkt dieses Erkennungsprozesses sind so genannte „Lightweight-Erkennungssensoren“, die auf dem Data Center Reference Model aufbauen und umfassend Infrastrukturkomponenten sowie deren Konfigurationen und Abhängigkeiten erkennen. Erkennungssensoren verwenden für die Erkennung der Komponenten im Rechenzentrum offene und sichere Protokolle und Zugriffsmechanismen. Darüber hinaus werden Erkennungssensoren im Gegensatz zu persistenten und invasiven Agenten zentral implementiert und verwaltet und beanspruchen nur wenig Bandbreite und CPU-Ressourcen (< 1 % im aktiven Modus) in der Zielumgebung. Die Discovery-Engine stellt einen Workflow-Framework für die Planung, Verteilung, Koordination und Verwaltung der verschiedenen Erkennungssensoren bereit.

Voraussetzungen für den Erkennungsprozess

Der Erkennungsprozess in TADDM erfordert minimale Konfigurationsinformationen:

- Erkennungsbereich: In der Regel wird hier ein gültiger IP-Bereich, ein Teilnetz oder eine Adresse angegeben. Der Erkennungsbereich gibt den Bereich für den Erkennungsprozess an.
- Zugriffslisten: Zugriffslisten geben die Berechtigungsnachweise für den Lesezugriff an, die für die Erkennung und Abfrage der Komponenten nach deren Konfigurationsattributen und Abhängigkeiten benötigt werden. Der Zugriffsmechanismus variiert je nach erkanntem Komponententyp. Beispiel:
    - SNMP-Communityzeichenfolgen zur Erkennung der Netzwerkelemente
    - SSH (Secure Shell) zur Erkennung der Konfiguration und Abhängigkeiten der UNIX-Hosts/ -Betriebssysteme
    - WMI (Windows Management Interface) zur Erkennung des Windows Betriebssystems und dessen Anwendungen
    - Protokolle wie JMX, SQL, LDAP und andere Standardzugriffsmechanismen zur Erkennung von Anwendungssoftware
- Zeitplandaten: Der TADDM-Erkennungsprozess kann bedarfsorientiert im Rahmen eines festgelegten Zeitplans oder durch extern ausgelöste Ereignisse ausgeführt werden.

Der Erkennungsprozess

Nach der Einleitung des Erkennungsprozesses führt die TADDM-Discovery-Engine mehrere Schritte aus:

- Die Discovery-Engine verwendet für die Prüfung des definierten Erkennungsbereichs Standardprotokolle, um die IP-Knoten (Adresse) aller installierten Einheiten zu erkennen.
- Für jeden gültigen IP-Knoten startet TADDM einen Erkennungssensor. Die Erkennungssensoren erkennen und kategorisieren die Komponententypen, indem sie sie den jeweiligen Signaturen im Data Center Reference Model zuordnen.

- Die Erkennungssensoren fragen dann die Komponente nach deren Konfiguration und Abhängigkeiten ab.
- Der Erkennungsprozess ist iterativ; jeder Erkennungssensorlauf kann einen nachfolgenden Erkennungssensor starten (z. B. wird durch eine Hosterkennung die Erkennung von Anwendungen und Services ausgelöst, die sich auf diesem Host befinden), bis die gesamte Infrastruktur vollständig erkannt ist.
- Nach Abschluss des Erkennungsprozesses verarbeitet TADDM die Daten der erkannten Komponenten und füllt damit die Configuration Management-Datenbank und generiert darüber hinaus eine topologische Darstellung der Infrastruktur.
- Durch nachfolgende Erkennungsläufe werden die Datenbank und die Topologien aktualisiert. Gleichzeitig wird ein umfassendes Änderungsprotokoll der Infrastrukturkonfiguration und der Abhängigkeiten erstellt und gepflegt.

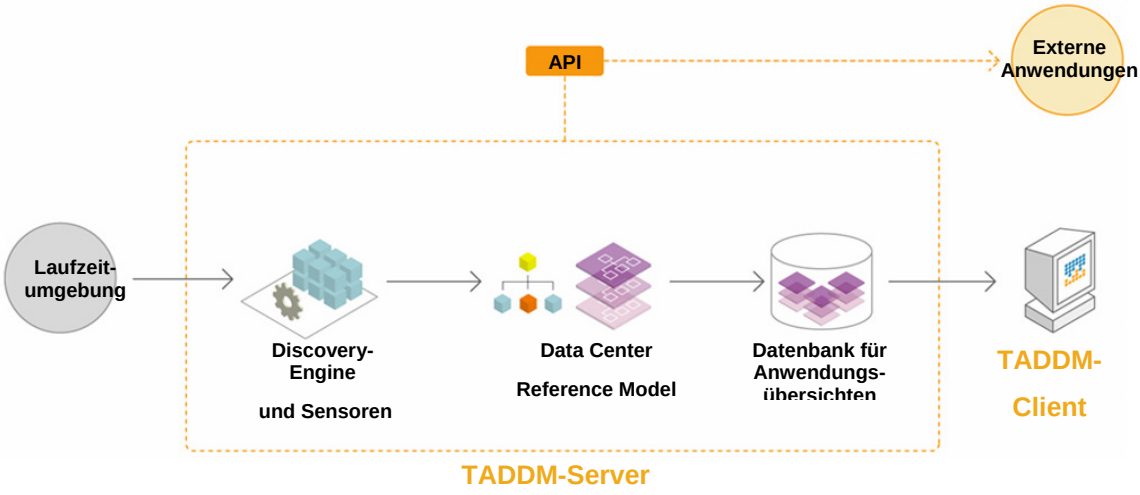


Abb. 2 Funktionsweise von TADDM

3.3 Erweiterbarkeit des Erkennungsprozesses

IBM bietet mit seiner TADDM-Lösung die umfassendste, sofort einsatzfähige Erkennungslösung auf dem Markt. Jedes Rechenzentrum hat jedoch über die bereits in die TADDM-Anwendung integrierten Anforderungen hinaus ganz individuelle oder neue Anforderungen. Um auch auf diese speziellen Anforderungen eingehen zu können, kann der TADDM-Erkennungsprozess auf drei Arten erweitert werden:

- **Angepasste Softwarekomponenten**: Alle aktiven angepassten Softwareprozesse werden sofort von TADDM erkannt. Diese erkannten Prozesse können danach gemäß ihren Laufzeitsignaturen identifiziert und

kategorisiert werden. So stehen sie auch für Konfigurationsprozesse, Änderungsverfolgung und Geschäftsservice-Erkennung zur Verfügung. Diese angepassten Serverschablonen lassen sich innerhalb weniger Minuten vom Benutzer über die TADDM-Benutzerschnittstelle und die APIs erstellen.

- **Sofort einsatzfähige Komponenten**: Alle Komponenten im Rechenzentrum, die zur Zeit nicht von den vorhandenen TADDM-Erkennungssensoren unterstützt werden, können innerhalb weniger Wochen von der IBM Sensor Factory erstellt werden. Die IBM Sensor Factory setzt sich aus flexiblen Ressourcen zusammen, über die kurzfristig neuen Sensoren unabhängig vom TADDM-Releasezyklus erstellt, getestet und ausgeliefert werden können. Die IBM Sensor Factory erstellt basierend auf der Nachfrage durch den Kunden kontinuierlich neue Sensoren.

- **Vorhandene oder angepasste Datenquellen**: Bei vielen Kunden sind die Konfigurationsdaten in Quellen wie Spreadsheets, Dateien oder anderen Tools enthalten. Der IBM Universal Data Sensor (UDS) erlaubt in solchen Fällen den zeitlich geplanten Import und die Transformation dieser Daten in das TADDM-Modell im Rahmen des Erkennungsprozesses. Dadurch kann TADDM vorhandene Datenquellen und Managementprozesse nutzen.

3.4 Erkennungsprozess bei Geschäftsanwendungen

In den heutigen Komponentenarchitekturen setzen sich Geschäftsanwendungen aus zahlreichen, in Wechselbeziehung zueinander stehenden Softwarekomponenten zusammen. Zur Zeit gibt es keine standardisierte Vorgehensweise für die Teams aus den Bereichen Prozessausführung und Servicebereitstellung, um feststellen zu können, welche Softwarekomponenten Teil einer bestimmten Geschäftsanwendung sind. IBM TADDM bietet in diesem Zusammenhang zwei Möglichkeiten, um diese Geschäftsanwendungsgruppierungen automatisch zu erstellen und zu verwalten:

1) IBM Application Descriptors
IBM Application Descriptors automatisieren den Prozess des Erstellens und Verwaltens von Geschäftsanwendungen. Dabei können Entwickler oder Implementierungsverantwortliche einfach aufgebaute XML-Dateien zu Anwendungsmodulen hinzufügen – und zwar zum Zeitpunkt der Zusammenstellung der Module und noch vor deren Implementierung. Über diese Anwendungsdeskriptoren kann TADDM dann automatisch die Geschäftsanwendungsgruppierungen erstellen und verwalten. Ein Beispiel für eine solche Anwendungsdeskriptordatei ist in Abbildung 3 dargestellt.

```
<base-app-descriptor>
    <app-instance
    name="Order Management - Staging"
    version="1.5.1"
    description="Order Entry application - staging"
    url="http://orderentry.stage.lab.com"
    contact="John Public" />
    <app-definition
    name="Order Management"
    description="Order Entry & Tracking application" />
```

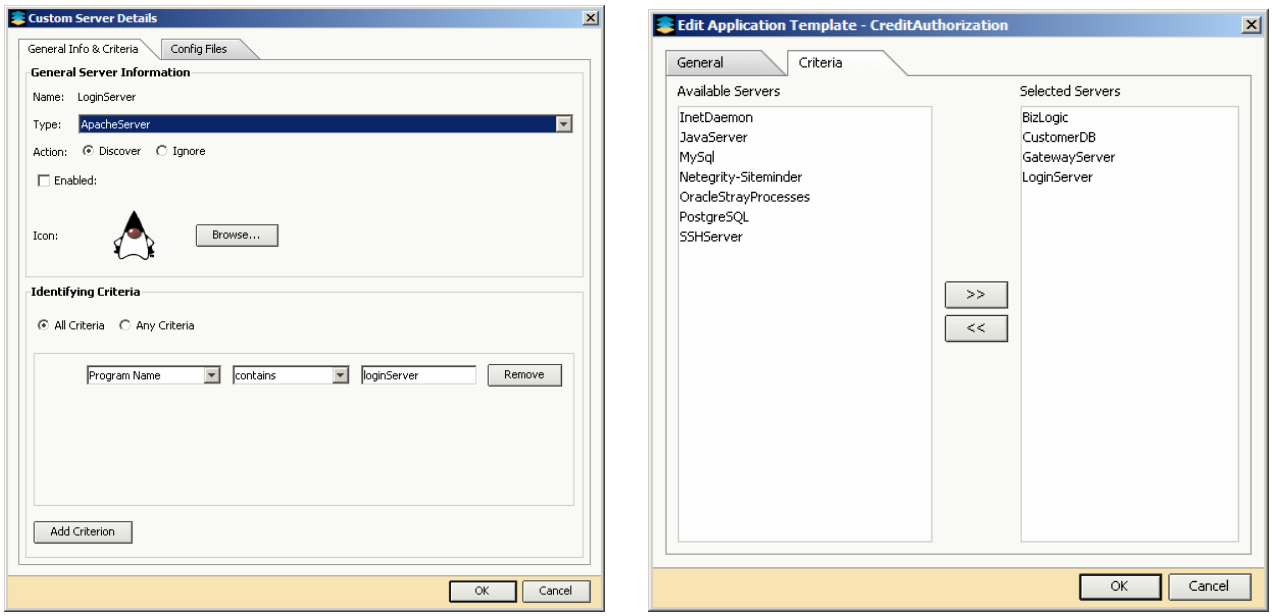
```
<component-app-descriptor
app-instance-name="Order Management-Staging">
<component-descriptor
type="module"
name="/opt/apache13/htdocs/ordermgt/"
functional-group="Web Tier"
marker-module="false" />
</component-app-descriptor>
```

Abb. 3: IBM Application Descriptors sind einfach aufgebaute XML-Dateien, in denen Geschäftsanwendungen und deren Komponenten definiert sind.

2) Schablonen für Komponenten- und Anwendungssignaturen

Neben den Anwendungsdeskriptoren kann TADDM Geschäftsanwendungen auch durch Identifizierung der Komponentensignaturen erkennen und übereinstimmende angepasste Komponenten als zu einer bestimmten Geschäftsanwendung oder einer anderen Anwendung gehörig zuweisen. Die Komponentenschablonen geben die eindeutige Signatur der Komponenten an, indem Kombinationen von Elementen wie Programmnamen, Ports und Umgebungsvariablen für die Klassifizierung der Komponenten herangezogen werden. Nach der Klassifizierung werden in der Geschäftsanwendungsschablone die Komponenten angegeben, die zu der jeweiligen Geschäftsanwendung gehören. Die Komponenten werden dann automatisch während des Erkennungsprozesses klassifiziert und gruppiert. Repräsentative Komponenten- und Anwendungsschablonen sind in Abbildung 4 dargestellt.

Hierzu folgendes Beispiel: Bei der Implementierung einer Anwendung für Kreditbewilligungen, die sich aus vier Komponenten zusammensetzt – LoginServer, Gateway-Server, BizLogic-Server und Kundendatenbank –, kann TADDM die Komponenten- und Anwendungsschablonen für die automatische Anwendungserkennung heranziehen. Basierend auf den eindeutigen Signaturen der einzelnen Komponenten (beispielsweise eine Apache-Anwendung, deren Programmname die Zeichenfolge „loginserver“ enthält) erkennt TADDM die Server und klassifiziert diese als übereinstimmend mit den jeweiligen Komponentenschablonen. Basierend auf der Anwendungsschablone fügt die Discovery-Engine die klassifizierten Komponenten der Topologie der Geschäftsanwendung für Kreditbewilligungen hinzu. Dadurch müssen Anwendungsgruppierungen nicht mehr manuell definiert werden. Die Komponenten- und Anwendungssignaturschablonen sind in Kombination mit den IBM Application Descriptors implementierbar.



.

Abb. 4: In angepassten Komponenten- und Anwendungsschablonen sind die Komponentensignaturen und die Anwendungszugehörigkeit definiert.

4. TADDM-Schnittstellen

4.1 Offene Schnittstellen in TADDM

Die TADDM-API ist eine sichere und modulare Schnittstelle zur TADDM-Datenbank. Die offene und veröffentlichte API bietet zahlreiche Bindings wie Java, Web Services/SOAP und Shell-Scripts. TADDM erzwingt den authentifizierten API-Zugriff, so dass nach der Authentifizierung allen API-Clients Zugriffsberechtigungen zugewiesen werden, wodurch wiederum Benutzeraktionen autorisiert werden. Darüber hinaus lässt sich der API-Zugriff über SSL verschlüsseln, so dass eine maximale Sicherheit gewährleistet ist. Die TADDM-API bietet das folgende Funktionsspektrum:

- **Daten-APIs:** Bieten Zugriff auf alle Anwendungstopologien einschließlich der Komponenten, deren detaillierte Konfigurationen sowie deren Abhängigkeiten zur Laufzeit. Die Daten-APIs erlauben zudem den Zugriff auf die TADDM-Funktionen für Änderungsanalyse und Berichterstellung. Darüber hinaus ermöglichen die Daten-APIs den Import und die Speicherung zusätzlicher Daten zu erkannten Komponenten wie Bestands-, Finanz- und Verwaltungsdaten.

- **Steuerungs-APIs:** Bieten asynchronen Zugriff auf die TADDM-Erkennungsprozesse einschließlich Erkennungskonfigurationen sowie Erkennungszeitplan und -steuerung. Mit Hilfe dieser APIs können auch Lösungen anderer Anbieter den TADDM-Server steuern. Hierzu gehört auch die Einleitung oder der Abbruch von Erkennungsläufen.

- **Ereignis-APIs:** Erlauben den Import von Ereignissen aus Lösungen anderer Anbieter in die TADDM-Anwendungstopologien sowie den Export von Änderungs- und Statusereignissen aus TADDM in Konsolen und Produkte anderer Anbieter.

Durch den Einsatz solcher APIs realisiert IBM sofortige Integrationsmöglichkeiten in Lösungen verschiedener führender Ökosystemanbieter wie Micromuse, Compuware, BMC Remedy, HP Openview und andere. Das TADDM-SDK umfasst Musterintegrationscode sowie Integrationstools, über die erfahrene XML-Programmierer problemlos angepasste Integrationen vor Ort vornehmen können.

4.2 Datenföderation in TADDM

Sobald Unternehmen IT Service Management-Initiativen in die Wege leiten, kommt auf IT-Manager die Anforderung zu, verschiedene Datenformen zu integrieren, damit für ein optimales Management der IT-Services verlässliche Informationen zur Verfügung stehen. So ist beispielsweise der CIO eines Unternehmens an den Gesamtinvestitionen in geschäftskritische Anwendungen interessiert, oder der CFO möchte sicherstellen, dass die

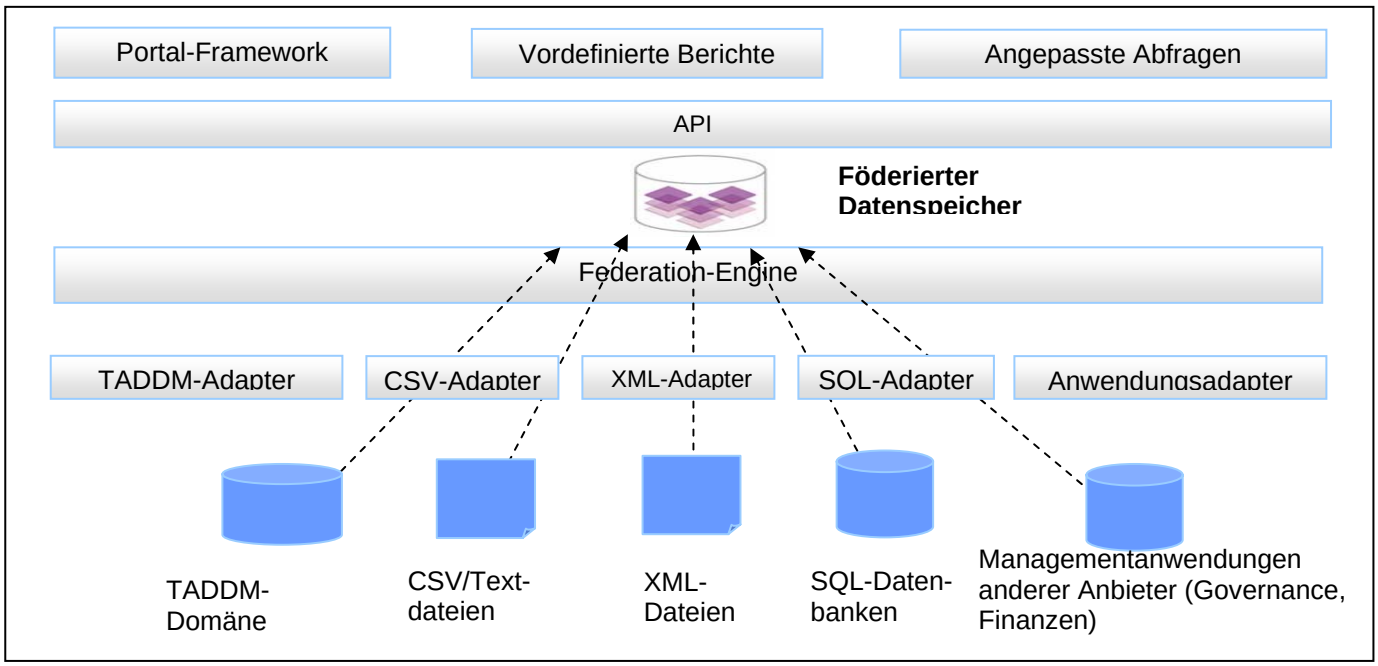
Finanzanwendungen alle behördlichen Vorgaben erfüllen. Um alle diese Wünsche und Anforderungen erfüllen zu können, müssen die IT-Manager verschiedene Datenformen konsolidieren und korrelieren:

- Informationen zur Anwendungsinfrastruktur (in Anwendungsübersichten)
- Informationen zu den Anwendungsressourcen
- Finanzdaten
- Benutzerinformationen zur Anwendung
- SLA-Messdaten

Heutzutage sind diese Daten in heterogenen Anwendungen zu finden und werden von unterschiedlichen Abteilungen im Unternehmen verwaltet. Außerdem können sich die Zugriffsteuerungsrichtlinien – wer erhält Zugriff auf welche Daten – und der Lebenszyklus der Anwendungsdaten – wie häufig werden die Daten aktualisiert – von Anwendung zu Anwendung gravierend unterscheiden. Die Brute-Force-Konsolidierung dieser Daten in ein zentrales Repository ist hierfür keine Lösung. Im Zusammenhang mit dieser Integrationsproblematik bei Unternehmensanwendungen bietet TADDM eine geradezu elegante Technologie für die Dateneinbindung. Anstatt die Daten in ein zentrales Repository zu konsolidieren, ermöglicht diese so genannte Föderationstechnologie in TADDM „Just-in-Time“-Zugriff auf diese Daten in den heterogenen Datenspeichern. Auf diese Weise können präzise und konsistente Berichte erstellt werden, die der IT-Abteilung einen hohen Nutzen bringen.

Die Föderationstechnologie in TADDM bietet folgende Leistungsmerkmale:

- Sofort einsatzfähige Adapter: Die TADDM-Föderationsplattform stellt sofort einsatzfähige Adapter für verschiedene Datenspeicher von Standardanwendungen wie XML-basierte Datenbanken, SQL-Datenbanken und CSV-/Textdateien bereit. Jeder Adapter speichert die Berechtigungsnachweise für die Zugriffsauthentifizierung für den Datenspeicher auf sichere Weise. Benutzer können nach Bedarf auch ihre eigenen angepassten Adapter erstellen.
- Federation-Engine: Über die Federation-Engine kann der Benutzer Regeln für den Zugriff auf den Datenspeicher erstellen, Filter bei der Suche nach Informationen (Zeilen oder XML-Daten) definieren und diese Datenströme „verknüpfen“ (korrelieren), um die gewünschten Berichte zu erstellen. Die Federation-Engine verfügt ebenfalls über einen API-Schnittstelle. Über diese Schnittstelle kann der Kunde Shell-Scripts/Java-Programme schreiben, um auf die eingebundenen Datenspeicher zugreifen und Berichte erstellen zu können.
- Berichtsportal: TADDM verfügt über ein webbasiertes Berichtsportal für Benutzer, über das die Berichte konfiguriert und angezeigt werden können. Dieses Portal entspricht JSR 168, sodass die Berichte problemlos innerhalb des Unternehmens gemeinsam genutzt werden können. Die Benutzer können die angepassten Berichte speichern und zu vorgegebenen Zeitintervallen aktualisieren, so dass die bereitgestellten Informationen immer den aktuellen Stand aufweisen.


Portal-Framework
Vordefinierte Berichte
Angepasste Abfragen
API
Föderierter Datenspeicher
Federation-Engine
TADDM-Adapter
CSV-Adapter
XML-Adapter
SQL-Adapter
Anwendungsadapter
TADDM-Domäne
CSV/Text-dateien
XML-Dateien
SQL-Daten-banken
Managementanwendungen anderer Anbieter (Governance, Finanzen)

5. Implementierungsarchitektur von TADDM

5.1 Typische TADDM-Implementierung und -Erkennung

Eine typische TADDM-Installation umfasst Folgendes:

- TADDM-Server: Der TADDM-Server wird unter Solaris 2.8 oder 2.9, Red Hat Enterprise Linux ES/AS 3.0 oder Suse 9 installiert. Die Mindestkonfiguration muss 2 CPUs (> 1,5 GHz), 2 GB RAM und 2 GB Plattenspeicherplatz umfassen
- TADDM-Datenbank: Oracle-Datenbankserver (8, 9, 10i/g) oder DB2 (UDB 8.2), die auf separaten Hosts/Servern implementiert werden
- TADDM-Clientkonsole: TADDM verwendet einen browserbasierten Client und erfordert keine separate Installation auf Kundenseite. Der TADDM-Client verwaltet den TADDM-Server und ist das Benutzerportal für die Analyse der Übersichten mit den erkannten Anwendungen.

5.2 Erkennung von Windows-Infrastrukturen

TADDM verwendet das sichere WMI-Protokoll (Windows Management Interface) für die Erkennung der Windows-/.NET-Anwendungsinfrastruktur. TADDM erfordert hierfür einen dedizierten Windows-Gateway-Server, der die Erkennungsprotokolle des TADDM-Servers zum WMI-Protokoll weiterleitet, um die ferne Windows-Infrastruktur erkennen zu können. Für die Windows-Gateway-Server gelten die folgenden Anforderungen:

- Windows 2003-Server mit einer Mindestkonfiguration von 2 GB RAM, 2 CPUs, 1,5-GHz-CPU, 600 MB freier Plattenspeicherplatz
- Netzwerkkonnektivität mit WMI-Zugriffsmöglichkeit auf alle fernen, für den Erkennungsprozess vorgesehenen Windows-Systeme mit Berechtigungsnachweisen für lokalen Administratorzugriff
- SSH-Software für die Kommunikation zwischen TADDM-Server und Windows-Gateway

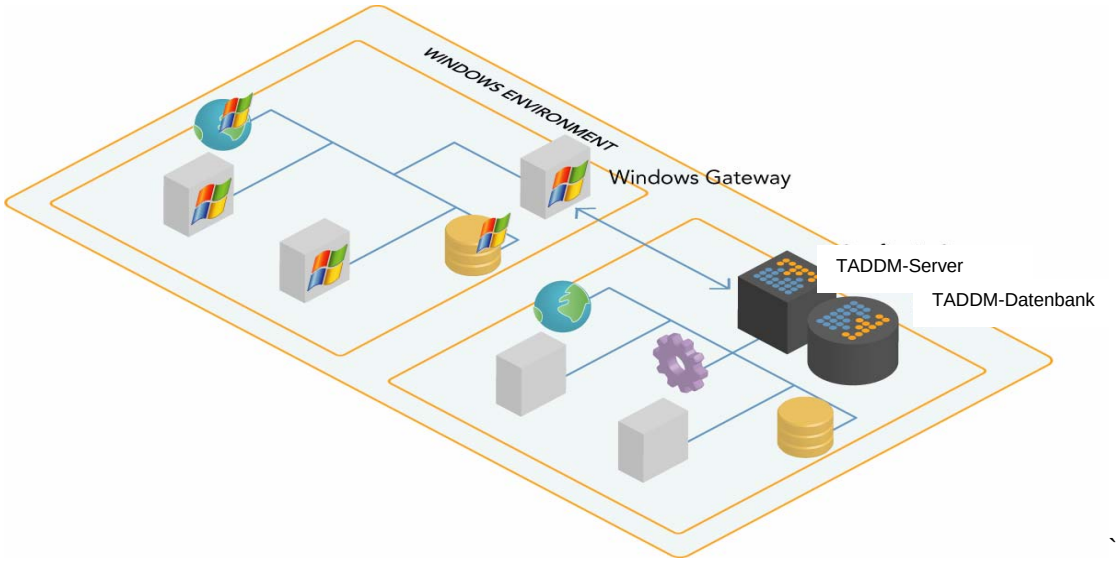


Abb. 5. TADDM-Architektur für die Erkennung von Windows-Infrastrukturen.

5.3 Transparente TADDM-Erkennung über Firewallzonen hinweg

Die TADDM-Basisimplementierung erfordert Netzwerkzugriff auf alle Infrastrukturelemente innerhalb des angegebenen IP-Bereichs. Einige Anwendungen können jedoch auch Firewallzonen umspannen, wenn Elemente einer Anwendungsinfrastruktur durch eine Firewall voneinander getrennt sind. Kundenorientierte Webanwendungen beispielsweise werden zusammen mit einem Web-Server-Cluster in einer DMZ (Demilitarized Zone) mit einer Firewall implementiert, die die DMZ von der Back-End-Geschäfts- und Prozessanwendung trennt. Aus Sicherheitsgründen erlauben die meisten IT-Richtlinien in den Unternehmen kein Öffnen von Ports in Firewalls. Einige Unternehmen implementieren zudem restriktive Filterrichtlinien, um den Netzwerkzugriff zu blockieren und eine sichere Kommunikation zu gewährleisten.

Das Design der TADDM-Implementierungsarchitektur ist so ausgelegt, dass in solchen Umgebungen ein einfaches und sicheres Arbeiten möglich ist. Um Anwendungen erkennen zu können, die sich über mehrere Firewallzonen erstrecken, setzt TADDM auf transparente und automatische Weise so genannte „Ankerserver“ in den Firewallzonen ein. Solche Ankerserver sind in der Lage, Anwendungsinfrastrukturen in den Firewallzonen zu erkennen. Der Benutzer muss nur einen sicheren SSH-Port in der Firewall öffnen, um Informationen zu und vom zentralen TADDM-Server zum angegebenen Ankerserver zu leiten. Der zentrale TADDM-Server konsolidiert die Daten vom Ankerserver und bietet so eine umfassende, firewallübergreifende Sicht der Anwendungsinfrastruktur.

Für TADDM-Ankerserver gelten die folgenden Voraussetzungen:

- Solaris 2.8 oder 2.9, Red Hat Enterprise Linux ES/AS 3.0 mit einer Mindestkonfiguration von 2 CPUs (> 900 MHz), 2 GB RAM und 800 MB Plattenspeicherplatz
- SSH-Software für die Kommunikation mit dem zentralen TADDM-Server
- Netzwerkkonnektivität zu den fernen Servern innerhalb des Erkennungsbereichs in der Firewallzone

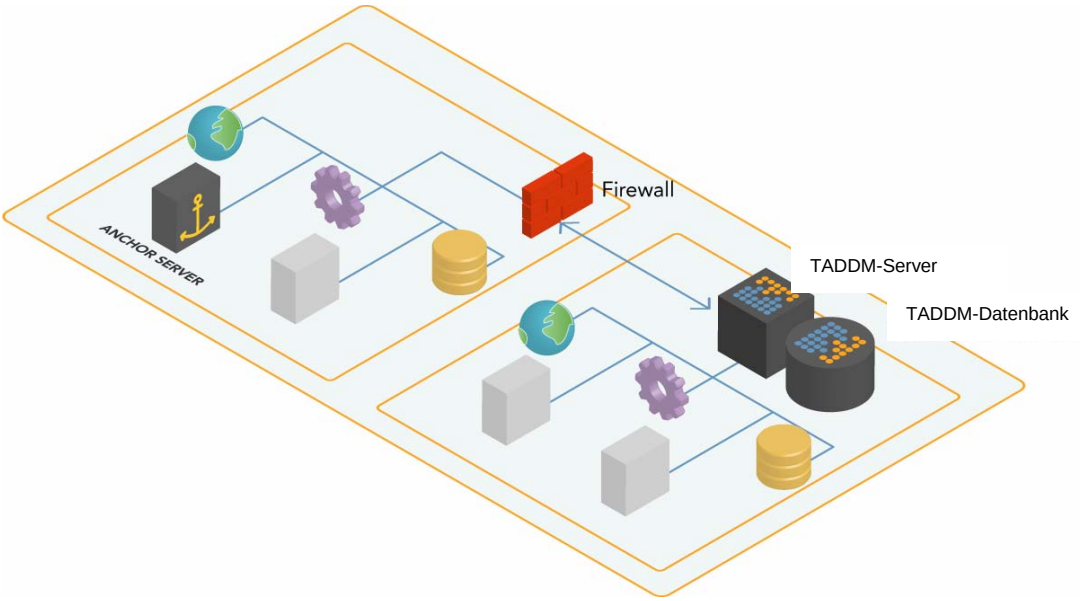


Abb. 6. TADDM kann über transparente Ankerserver auch in Firewallzonen effizient eingesetzt werden.

5.4 TADDM-Skalierbarkeit für unternehmensweite Transparenz

Die Architektur von TADDM ist so ausgelegt, dass eine modulare Skalierung für große Rechenzentren erfolgen kann. Ein einzelner TADDM-Server kann ca. 10.000 physische Server unterstützen (ein einzelner physischer Server kann mehre Software-Server bedienen und mit mehreren Netzwerkeinheiten verbunden werden). Der Kunde hat zudem die Möglichkeit, die TADDM- Betriebsmerkmale (z. B. Threadzähler der Discovery-Engine, Zeitlimitüberschreitungen bei Erkennungssensoren usw.) zu optimieren und die TADDM-Server- oder TADDM-Datenbankressourcen (CPUs, Speicher usw.) zu erhöhen, um die Infrastrukturerkennung und Speicherprozesse noch besser unterstützen zu können.

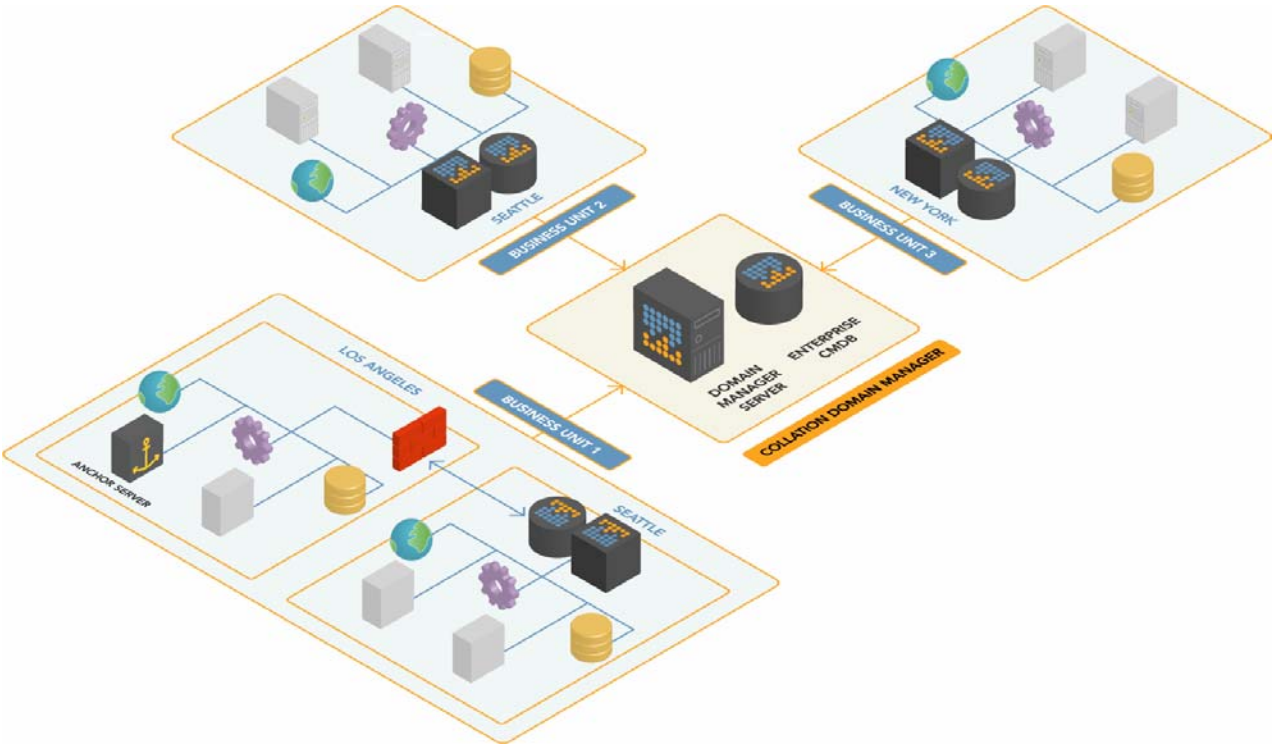


Abb. 8. TADDM bietet Best Practices für eine äußerst elegante „domänenbasierte“ Skalierbarkeit und unterstützt so auch außergewöhnlich umfangreiche Implementierungen auf Unternehmensebene.

TADDM-Server können so skaliert werden, dass sie auch komplexe und umfangreiche Unternehmensumgebungen unterstützen. IBM bietet hierfür eine „domänenbasierte”, auf Best Practices aufbauende Implementierungsarchitektur, um auf geradezu elegante Weise eine optimale Skalierbarkeit der Lösung sicherzustellen, damit auch Zehntausende von Infrastrukturelementen problemlos unterstützt werden können.

Sehr umfangreiche Infrastrukturen werden in so genannte „Managementdomänen“ unterteilt, die die Steuerungsbandbreite eines IT-Teams angeben. Solche Domänen können auf unternehmensweiten, funktionalen oder geografischen Grenzen oder einer Kombination daraus bzw. auf anderen Kriterien aufsetzen. Um diese betrieblichen Anforderungen der Domäne ausreichend zu unterstützen, empfiehlt IBM pro Managementdomäne einen eigenständigen TADDM-Server. Jeder TADDM-Server ist so für seine eigene Domäne zuständig – der Server erkennt und speichert alle Konfigurationsdaten für seine lokale Domäne. Die Benutzer jeder Managementdomäne verwendet die lokale TADDM-Instanz für das Management der prozessbezogenen Aspekte ihrer Domäne. Hierzu gehören auch die Ausführung von Analysen wie die Erstellung von Änderungsprotokollen, Vergleichsläufen und Bestandsberichten. In Abbildung 8 beispielsweise führt ein TADDM-Domänenserver Zuordnungen durch und verwaltet die einzelnen Rechenzentren in Seattle, Los Angeles und New York.

Unabhängig davon müssen IT-Unternehmen auch domänenübergreifende Sichten ihrer IT-Informationen verfügbar haben. Für den CIO ist es beispielsweise wichtig, einen Ergebniswert seiner unternehmensweiten Oracle-Implementierungen verfügbar zu haben, um die Einhaltung der Lizenzverträge sicherzustellen. Diese Funktionalität stellt IBM TADDM Domain Manager zur Verfügung. TADDM Domain Manager föderiert die Daten aus verschiedenen lokalen TADDM-Serverinstanzen und stellt ein „konsolidiertes“ zentrales und unternehmensweites Informationsrepository bereit. Diese Föderationsarchitektur stellt sicher, dass die Daten in verschiedenen Datenspeichern nicht doppelt vorkommen – TADDM Domain Manager speichert Referenzen zu den betreffenden Daten im lokalen TADDM-Server und greift nach Bedarf auf die Daten zu.

IBM TADDM Domain Manager verfügt darüber hinaus über ein Webportal, über das die lokalen Domänenserver verwaltet und die konsolidierten Unternehmensdaten angezeigt und analysiert werden können. Die anpassbare Abfrage- und Berichtsschnittstelle erlaubt die einfache gemeinsame Nutzung der Daten im gesamten Unternehmen.

6. TADDM-Sicherheit

Im Gegensatz zu anderen Lösungen setzt der TADDM-Erkennungsprozess nicht die Implementierung persistenter Agenten in der Zielumgebung voraus. Durch diesen Ansatz entfällt nicht nur die Qualifizierung und das Management weiterer Agenten; auch die mit der Implementierung persistenter Agenten in der Rechenzentrumsinfrastruktur verbundenen Sicherheits- und Supportrisiken entfallen. Die TADDM-Erkennungssensoren verwenden für die Erkennung der Infrastrukturkomponenten und deren Konfigurationen auf Branchenstandards basierende sichere Protokolle. Der TADDM-Erkennungsprozess baut auf Secure Shell Protocol (SSH)[4] auf, dem so genannten „Goldenen Standard" für die sichere, unternehmensweite Kommunikation im Rechenzentrum. TADDM setzt SSH sehr umfassend für die strikte Authentifizierung und Verschlüsselung während des Erkennungsprozesses ein. Darüber hinaus erfordert TADDM nur Lesezugriff und keine Schreibberechtigungen.

TADDM gewährleistet zudem den sicheren Zugriff auf seine Server und die Datenbank für Anwendungsübersichten. Der Zugriff auf den TADDM-Server wird nur für Benutzer oder Anwendungen mit gültigen Anmelde-/Kennwortdaten ermöglicht. TADDM unterstützt und empfiehlt die zertifikatbasierte Authentifizierung über ein SSL-Protokoll – und zwar für Benutzer- und API-Clients. Nach der erfolgreichen Authentifizierung werden dem Benutzer sowohl mehrschichtige Rollen mit Leseberechtigungen als auch Berechtigungen für Erkennungsaktionen zugeordnet. Außerdem werden basierend auf dem authentifizierten Zugriff auf den TADDM-Server alle Benutzeraktionen für Prüfzwecke verfolgt, protokolliert und für den autorisierten Zugriff bereitgestellt. Die wichtigsten TADDM-Sicherheitsfunktionen sind in der folgenden Tabelle zusammengefasst.

Feature	**Vorteile**
Agentenfreie Erkennung	Wegfall von langwierigen und kostspieligen Qualifizierungsprozessen und von Risiken bei der Instrumentierung von Betriebssystemen und Code
Einsatz von SSH für den Hostzugriff	Authentifizierung und Sicherung aller Erkennungsaktivitäten
Nur Lesezugriff erforderlich	Verhinderung unberechtigter Aktionen bei erkannten Komponenten
Vollständige Protokollierung der Benutzeraktivitäten	Ermöglicht zuverlässige Sicherheitsprüfungen
Berechtigungsnachweise für Benutzer- oder API-Zugriff erforderlich	Kein unberechtigter Zugriff auf Informationen oder Steuermechanismen
Automatische Implementierung von Ankerservern	Nahtlose Erkennungsaktivitäten über Firewallzonen hinweg

4 http://www.ietf.org/html.charters/secsh-charter.html und http://www.openssh.com/

7. Schlussfolgerung

Die IBM TADDM-Lösung zur Erstellung von Anwendungsübersichten ist ein unternehmensweit einsetzbares Lösungsangebot, das auf einem standardbasierten Data Center Reference Model aufbaut. Das Produkt führt agentenfreie Erkennungsprozesse für die gesamte schichtübergreifende Anwendungsinfrastruktur durch und ???speist diese Informationen über das Referenzmodell ein. Dadurch werden spezielle Anwendungsübersichten erstellt, die in einer entsprechenden Datenbank verwaltet werden. Diese enthält Informationen zu allen Komponenten einer Anwendung und den Abhängigkeiten während der Laufzeit sowie detaillierte Angaben zu den Konfigurationseinstellungen. Diese Informationen und die Änderungen dieser Informationen werden in einer erweiterbaren und offenen Datenbank gespeichert.

TADDM bietet umfassende Daten-, Steuerungs- und Ereignis-APIs, damit diese Informationen auch von vorhandenen und kommenden Managementprodukten und -prozessen verwendet werden können. Diese APIs werden durch ein umfassendes und auf Standards basierendes Software Development Toolkit (SDK) unterstützt, wodurch IT-Abteilungen auch kurzfristig die erforderlichen Integrationsmaßnahmen implementieren können.

TADDM bietet sowohl horizontale als auch vertikale Skalierungsmöglichkeiten und kann flexibel sowohl in Management- als auch Sicherheitsdomänen implementiert werden. Um alle möglichen Kombinationen aus Management- und Sicherheitsanforderungen abdecken zu können, kann die Implementierungsarchitektur von TADDM ganz individuell an die Anforderungen jedes Unternehmens angepasst werden. Das Design von TADDM ist zudem so ausgelegt, dass es alle Anforderungen der Unternehmen nach Zuverlässigkeit und Sicherheit erfüllt.

Insgesamt gesehen ist TADDM eine erweiterbare, skalierbare und sichere Lösung, die umfassende Transparenz und Einblicke in komplexe Anwendungsinfrastrukturen bietet. Durch die Implementierung von TADDM können Unternehmen die Verfügbarkeit, Konsistenz und Flexibilität bei der Bereitstellung von Services für ihre geschäftskritischen Anwendungen deutlich verbessern.

8. Referenzen und interessante Sites

8.1 Referenzen

Enterprise Management Associates, „The ITIL Configuration Management Database: Panacea or Pandora's Box?“, Dezember 2004

Forrester (Mendel, Parker), „Not all ITIL Processes are Created Equal”, 16. März 2005

Gartner (Adams, Colville), „Defining a Configuration Management Database“, 15. November 2004/ID-Nummer: G00123937

Gartner (Colville), „Organizations Are Paying More Attention to Configuration Management“, 31. März 2005

8.2 Interessante Sites

www.dmtf.org – Homepage zum CIM II-Standard

www.jcp.org/en/jsr/detail?id=77 – Informationen zur Verwaltbarkeit von JSR77 und J2EE

www.itsmfusa.org/ – Das IT Service Management Forum

www.ogc.gov.uk/index.asp?id=2261 – Ausgangspunkt von ITIL, der IT Infrastructure Library

www.ietf.org/html.charters/secsh-charter.html – Informationen zu Secure Shell

www.openssh.com/ – Zugriff auf OpenSSH-Produkte und Informationen

8.3 Sites von Branchenanalysten

www.gartner.com

www.forrester.com

www.summitstrat.com

www.enterprisemanagement.com/