



alcatrass Secure System Management

Überblick

- alcatrass ist eine Plattform für **Security- und System Management**
- alcatrass bietet ein besonders modernes und effizientes Plattform-Konzept für zentrale Security- und System Management Aufgaben in **komplexen und heterogenen Netzwerken und IT –Systemlandschaften**
- alcatrass wurde mit den Prämissen **Sicherheit, Flexibilität, Standardisierung und Kosten/Nutzen** konzipiert

alcatrass
secure system management





alcatrass Secure System Management

Überblick

alcatrass
secure system management



alcatrass...

- ... kann alle Informationsquellen überwachen
- ... überwacht und steuert gezielt Systeme und Informationen die für eine spezifische IT-Umgebung erforderlich ist
- ... ist nicht hoch komplex und leicht zu implementieren



Der Tradeoff

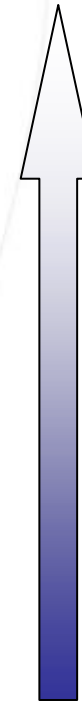
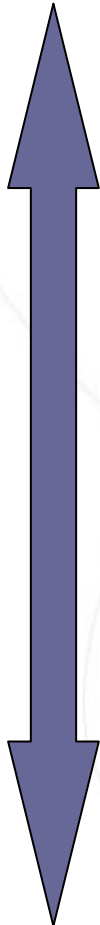
„Hohe Integration vs. Plattform“

Hoch integrierte Tools

- (Sehr) viele, qualifizierte Daten
- Hoch spezialisierte Aufgabengebiete
- Hohe Kosten
- Hohe Aufwendungen bei Konzeption und Implementierung
- Ressourcenaufwendig
- Geringe Flexibilität
- Proprietär

Plattform-Lösung

- Geringe Kosten
- Geringe Aufwendungen bei Konzeption und Implementierung
- Hohe Flexibilität
- Universell einsetzbar
- Schnell, Ressourcenschonend
- geringere Datenfülle möglich
- Höhere Sicherheit
- Standardisiert



alcatrass



alcatrass Secure System Management

Die Entscheidung

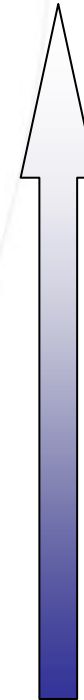
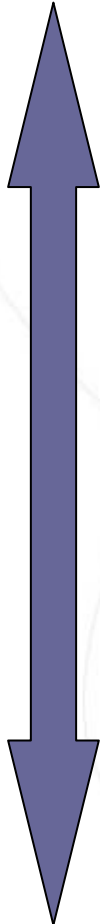
Kosten / Nutzen

Hoch integrierte Tools

- viele, qualifizierte Details
- Großer Funktionsumfang
- Hohe Kosten
- Aufwand für jedes spezifische System

Plattform-Lösung

- Geringe Kosten und Aufwendungen
- Für alle Systeme
- Ist die Datenfülle erforderlich?



alcatrass



alcatrass Secure System Management

Funktionalität Überblick

1. Mit **alcatrass** können **alle erforderlichen Funktionen für Security- und System Management Systeme** implementiert werden
2. **alcatrass** setzt auf **System-Standards** und läuft auf allen gängigen Systemen

alcatrass basiert **ausschließlich auf Webtechnologien**. Dadurch können alle Systeme eingebunden und über einen Browser (auch remote), überwacht, gesteuert, konfiguriert und administriert werden

3. **alcatrass** kann **alle erforderlichen Systeme** überwachen und steuern, insbesondere Standardsysteme
4. Eine **Erweiterung der Funktionalität** für zu überwachende oder zu steuernde Systeme erfordert **keine Programmierung**.



alcatrass Secure System Management

1. Funktionalität - alcatrass Funktionsumfang

Folgende Funktionen stellt **alcatrass** zur Verfügung:

- Überwachung von Systemen
- Steuerung von Systemen
- Alerting, Information
- Webbasierte Konfiguration und Administration
- Datenbank, Web- und LDAP Anbindung
- Zentrale Verarbeitung und Korrelation von Systemmeldungen
- Gesicherte, authentifizierte Übertragung
- Event-Routing
- Cachen von Daten

Diese Basisfunktionen bilden die Plattform für alle zentralen Security und System Management Aufgaben



alcatrass Secure System Management

2. Funktionalität - alcatrass System-Standards

alcatrass setzt konsequent auf Standards

- Interne Sprache: RegEx
- Konfigurationsdatenablage: LDAP
- Freie Datenbank: JDBC
- Betriebssystemunabhängig: Java

alcatrass nutzt standardisierte Komponenten und Schnittstellen und kann sich dadurch in jede Systemlandschaft integrieren.

Daraus ergeben sich weitere Eigenschaften, die eine Standardisierung der Lösungen mit **alcatrass** bewirken

- Keine Programmierung, nur Konfiguration ist nötig (RegEx)
- Keine Erweiterungen außerhalb der Standard-Mechanismen erforderlich
- **alcatrass** überwacht sich selbst mit den selben Mechanismen wie die anderen überwachten Systeme.

3. Funktionalität - alcatrass Überwachungsumfang

Alle gängigen Betriebssysteme

- Unix
 - HPUX
 - SUN Solaris
 - Linux (SuSE, RedHat, Debian, usw.)
 - AIX
 - weitere...
- Windows
 - 95, 98, XP, NT, 2000, 2003

Standardumfang der Überwachung:

- Syslogs
- Eventlogs
- SNMP
- Logfiles, Named Pipes, Sockets



alcatrass Secure System Management

3. Funktionalität - alcatrass Überwachungsumfang

Alle gängigen Datenbanken

- Relational
 - Oracle
 - MS SQL
 - DB2
 - Informix
 - mySQL
- Multidimensional
 - Hyperion Essbase
 - MS SQL OLAP
- Hierarchisch
 - Tamino (Software AG)
 - LDAP Datenbanken

Standardumfang der Überwachung

- Verfügbarkeit der Systemdienste
- Tablespace
- System-Logs, Error-Logs

3. Funktionalität - alcatrass Überwachungsumfang

Alle gängigen Netzwerkkomponenten

- Router, Switches

Standardumfang der Überwachung:

- SNMP
- Error Logs

Alle gängigen Security-Systeme

- Firewalls
- Intrusion Detection Systeme
- Virens Scanner

Standardumfang der Überwachung:

- Verfügbarkeit der Systemdienste
- Angriffe
- Aktualität von Signaturen

Hardware aus Rechenzentren

- USVs, Türkontakte, Rauchmelder, Wärmesensoren



alcatrass Secure System Management

4. Funktionalität - alcatrass ist einfach erweiterbar

Eine **Erweiterung der Funktionalität** für zu überwachende oder zu steuernde Systeme **erfordert keine Programmierung**. **alcatrass** nutzt die Standard Auszeichnungssprache RegEx (Reguläre Ausdrücke). Somit können gezielt Systeme und Parameter überwacht werden, die nicht als Standard-Umfang zu bezeichnen sind. Die Überwachung neuer Systeme und Parameter erfolgt mit den selben Mechanismen wie die Überwachung der Standards!!

Funktionalität Fazit:

- **alcatrass ist konzipiert, um sich auf die für die jeweilige Security- oder System Management-Lösung wichtigen Elemente zu konzentrieren.**
- **Dies sind meist die Standards mit einigen, wenigen Erweiterungen.**



alcatrass Secure System Management

Markt

- **alcatrass** hat keine typische Konkurrenz auf dem Markt
- **alcatrass** hat **keine Konkurrenzstellung zu hoch spezialisierten, proprietären Produkten** mit systemspezifischen Funktionsumfang.
-> **alcatrass unterscheidet sich:**
weniger hoher, spezifischer Standard-Funktionsumfang für die einzelnen Systeme, dafür Einbindung aller (weiterer) Systeme (und Systemplattformen) und freier Funktionsumfang.
- **alcatrass** hat **keine Konkurrenzstellung zu Enterpriseplattformen.**
Produkte, die system- und funktionsübergreifende Funktionalitäten wie **alcatrass** abdecken sind voluminös und aus vielen Proprietären, uneinheitlichen Komponenten zusammengesetzt.
-> **alcatrass unterscheidet sich:**
weniger hohe Integration, dafür klein, schnell, Ressourcen schonend und kostengünstig.
- **Es gibt kein Produkt auf dem Markt, dass das Plattform-Konzept so konsequent und umfassend wie alcatrass umsetzt.**



alcatrass Secure System Management

Historie, Entwicklung

- **alcatrass** wurde Ende 1997 in der Version V1.0 als scriptbasierte Systemüberwachung und Steuerung vorgestellt. Der Fokus der Funktionalität war die Absicherung von Netzwerken.
- Die Version 2.0 erweiterte den Funktionsumfang zu einem Security- und System Management System.
- Mit der Version 3.0 ist alcatrass voll webbasiert.
Das Release der **alcatrass** Version 3.0 am 15. November 2001 wurde von unserem bestehenden Kundenkreis sehr gut aufgenommen und ist z. B. bei der RegTP (Regulierungsbehörde für Telekommunikation und Post) und bei der Siemens AG (ICN) im Einsatz.
- Mit der Version 4.0 wurden alle **alcatrass** Komponenten auf Java umgestellt. Größere Teile der Systemadministration wurden in den WebCenter verlagert. Alle 3.0 **alcatrass** Installationen wurden bereits auf die Version 4.0 aktualisiert.
- Aktuell ist die Version 4.1 die auf der SYSTEMS 2003 vorgestellt wird.



alcatrass Secure System Management

Überlick USPs

alcatrass ist	Kundennutzen
Hersteller- und plattformunabhängig	alcatrass läuft auf allen gängigen Betriebs-, Datenbank- und Internetserver-Systemen. alcatrass kann überall implementiert werden -> einfache, schnelle und Ressourcenschonende Integration in die bestehende Systemlandschaft
Web basiert	Nur ein beliebiger Web Browser ist notwendig, keine Client Installation und keine Lizenzierung erforderlich!
Für heterogene IT Systeme, Strukturen und Netzwerke konzipiert	alcatrass ist Betriebssystem-, Datenbank- und Applikationsübergreifend einsetzbar; es gibt keine Einschränkungen bzgl. der Systeme und des Funktionsumfangs
Einfach erweiterbar und lernfähig	Einbinden weiterer Systeme und Funktionen ist schnell und einfach (und standardisiert) ohne Programmierung möglich. alcatrass erkennt auch unbekannte Informationen und kann so kontinuierlich erweitert und verbessert werden
Klein, schnell und günstig	alcatrass ist schnell und kostengünstig im Einsatz, keine aufwendigen Systemressourcen sind erforderlich.