

Access- und Sicherheitsmanagement

Zu den unbestrittenen Vorteilen eines organisationsweiten Access- und Sicherheitsmanagement zählen unter anderem die tägliche Zeitersparnis bei der Authentifizierung der Mitarbeiter, dadurch erzielte Kosteneinsparungen, schneller und sicherer Return On Investment, verbesserte Benutzerfreundlichkeit und anwendungsübergreifende Sicherheit. Dementsprechend ist vor allem in größeren Organisationen des öffentlichen wie auch privaten Sektors die Einführung eines organisationsweiten Single Sign-On ein Thema. Die Einführung einer solchen Access-Management-Lösung ist jedoch gerade in Organisationen mit heterogener IT-Landschaft eine komplexe Herausforderung.

Cafesoft bietet Ihnen mit Cams eine äußerst flexible, linear skalierbare, höchsten Sicherheitsstandards entsprechende und zudem kostengünstige Lösung zum zentralen Access- und Sicherheitsmanagement mit Web Single Sign-On in Ihrer Organisation.

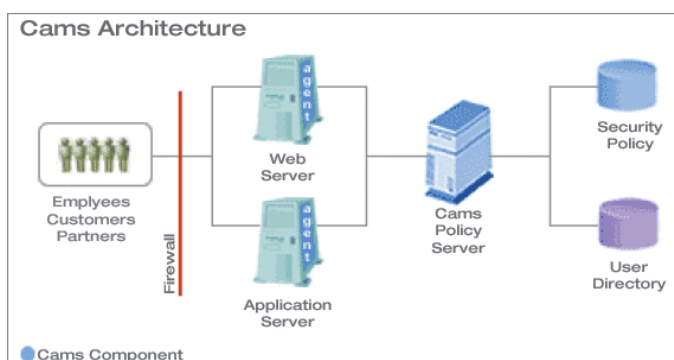


Die Cams-Architektur

Je nach IT-Umgebung und individuellen Anforderungen sind mit Cams™ unterschiedlichste Netzwerktopologien umsetzbar. Dabei können u.a. auch X500 Client-Zertifikate in das Sicherheitskonzept miteinbezogen werden. Eine Lösung mit Cams basiert dabei auf folgenden zwei Komponenten:

- Ein Cams™ - Policy-Server: Dieser dient als zentrale Instanz für alle Authentifizierungs- sowie Autorisierungsvorgänge und stellt die Verbindung zwischen allen Servern/Anwendungen und der Benutzerverwaltung, bzw. -datenbank dar.
- Ein Cams™ - Agent je zu schützende Anwendung/ Server: Aufgabe des Agenten ist es, jede ankommende Anfrage eines Anwenders/Nutzers zu prüfen und beim Policy-Server zu ermitteln, ob die gewünschte Aktion erlaubt ist.

In den unten gezeigten Schaubildern sind beispielhaft eine „einfache“ Cams-Architektur sowie eine typische Proxy Topologie gezeigt.

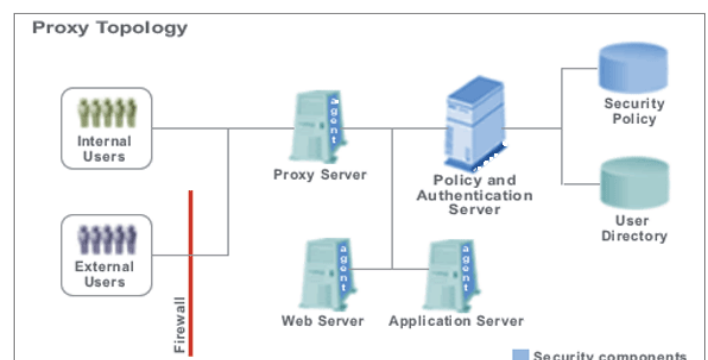
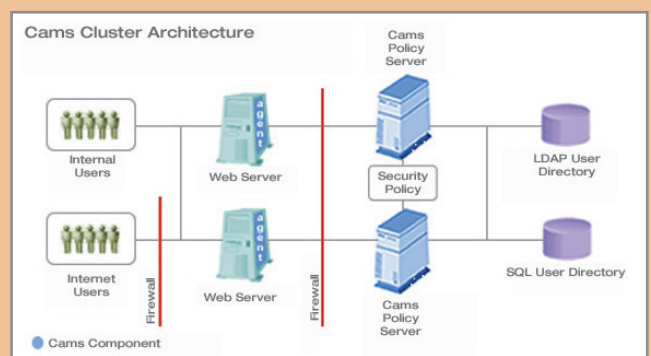


Web Single Sign-On in heterogenen IT-Umgebungen

Anwendungsübergreifende Sicherheit ist häufig nur mit den Produkten eines Herstellers problemlos möglich. In größeren Netzwerken kommen jedoch in der Regel unterschiedliche Anwendungen und Applikationsserver von verschiedenen Herstellern zum Einsatz. Zusätzlich dazu sollen oftmals auch Open Source Komponenten wie beispielsweise Apache, Tomcat oder JBoss eingesetzt werden. Dies ist genau die Problemdimension, an der Cams™ ansetzt: mit Hilfe von Cams™ kann herstellerunabhängig eine zentrale Benutzerverwaltung realisiert werden, mit der ein sicheres Single Sign-On über sämtliche Webinhalte und Webanwendungen in einer Organisation umgesetzt wird. So lassen sich auch Inhalte und Anwendungen, die auf Web- und Applikationsservern unterschiedlichster Hersteller liegen effizient schützen.

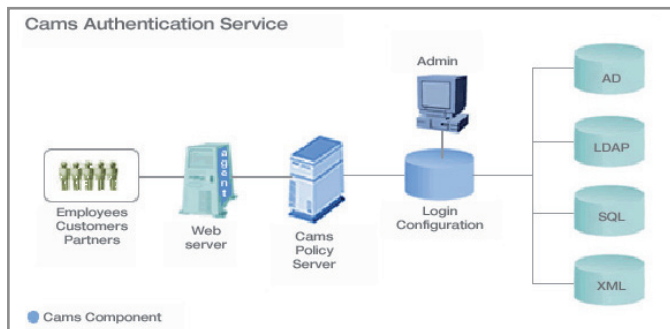
Cluster Architektur

- Ausschluß eines „Single Point Of Failure“ - fällt aus irgendwelchen Gründen ein Policy Server (vorübergehend) aus, so werden die Anfragen der Web Agents an den/die jeweils verbleibenden Policy Server umgeleitet und bearbeitet. Um darüber hinaus gegen des Ausfall weiterer Netzwerkkomponenten abgesichert zu sein, können die Policy Server eines Clusters in verschiedenen Netzwerkbereichen angesiedelt werden.
- Optimale Skalierbarkeit - bestehende Cluster können sehr einfach durch weitere Server/Instanzen vergrößert und ausgebaut werden. So lassen sich auch wachsende Zugriffszahlen und sonstige Anforderungen innerhalb komplexer Systeme problemlos abbilden.



Authentifizierung mit Cams

Die Implementierung dieser Cams™-Komponenten ermöglicht die sichere Authentifizierung der Benutzer, und das gegenüber einer unbestimmten Anzahl verschiedener Datenquellen, in welchen die Userdaten hinterlegt sind. Ebenso können damit die Rechte für eine prinzipiell unbegrenzte Anzahl von Applikationen gesteuert und verwaltet werden. So müssen beim Einsatz von Cams™ auch keine aufwendigen Migrationen oder der Aufbau gänzlich neuer Benutzerverwaltungen durchgeführt werden. Dabei verfügt Cams™ über Module für folgende (Benutzerdaten-) Datenquellen:



- Microsoft Active Directory
- LDAP-Server, wie z.B. Open LDAP, SunOne, etc.
- SQL-Datenbanken, wie z.B. Oracle 9i, My SQL, Microsoft SQL-Server, etc.
- Darüber hinaus wird mit Cams™ eine XML-File basierte Benutzerverwaltung mitgeliefert, die bei Bedarf zusätzlich eingesetzt werden kann

Cams™ - unterstützte Plattformen

CAMS™ ist äußerst flexibel einsetzbar und nicht an die Software-Produkte eines bestimmten Herstellers gebunden. Unterstützt werden folgende Plattformen:

Cams Policy Server:

- Mac OS X
- Mac OS X Server
- Red Hat Linux 7/8/9
- Red Hat Enterprise Linux
- Sun Solaris 8/9
- SuSE Linux 7/8/9
- Windows NT 4.0 Workstation und Server
- Windows 2000 Workstation und Server
- Windows 2003 Server
- Windows XP
- Weitere Betriebssysteme mit Java JRE 1.4.x

Cams Web Agents:

- Apache1.3 (Red Hat Linux 7/8/9)
- Apache 2.0.40 und 2.0.49 mit Red Hat 8/9
- Apache 2.0.49 mit Windows NT, Windows 2000, Windows Server 2003
- J2EE Applikationsserver via Servlet Filter
- BEA WebLogic 7/8
- IBM WebSphere 5
- JBoss 3.2.x mit Jetty/Tomcat
- Jetty 4.2.x
- Jrun 4.x
- Oracle 9iAS
- Tomcat 4/5
- Weitere J2EE Server, die Servlet API 2.3 unterstützen
- Microsoft IIS 4/5/6
- Netscape/SunOne 6.x mit Solaris 8/9
- Tomcat 4/5

Benutzerverwaltung (Directories):

LDAP:

- IBM Directory Server
- Microsoft Active Directory und ADAM
- Microsoft SiteServer LDAP Server
- Novell eDirectory
- OpenLDAP
- SunOne/iPlanet/Netscape Directory Server
- Weitere LDAP V.3-konforme Verzeichnisse

Datenbanken:

- HypersonicSQL
- IBM DB2
- Microsoft SQL Server
- MySQL
- Oracle 9i
- Sybase
- Weitere Datenbanken mit JDBC 2.0-Driver



Vertrieb und weitere Informationen:

SEITENBAU GmbH.

Seilerstraße 7. D-78467 Konstanz. Tel +49(0)75 31/3 65 98-00. Fax +49(0)75 31/3 65 98-11.

Hohenzollernring 52. D-50672 Köln. Tel +49(0)2 21/88 88 16-0. Fax +49(0)2 21/88 88 61-11.

info@seitenbau.com www.seitenbau.com www.cafesoft.de