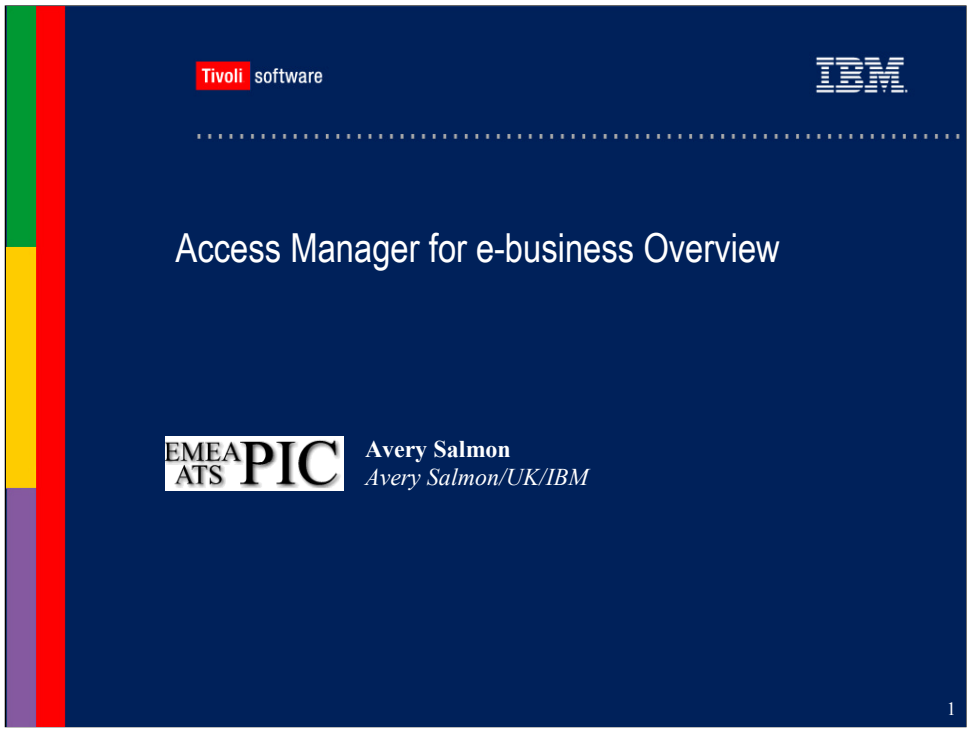


Policy Director has been renamed "IBM Tivoli Access Manager for e-business." This was announced on 9th April.

We have tried to replace all occurrences of 'Policy Director' in workshop material with 'Access Manager'. You may, however, still find 'PD' or 'Policy Director' in the material and/or the product. Please consider this to be Access Manager 3.9, unless the text explicitly says otherwise.

This intent of this overview is to give you a quick summary of the new features of Access Manager 3.9.

Agenda

EMEA ATS PIC

- Recent & Upcoming News
- Brief Overview
  - Packages,Platforms, Directories, pre-requisites
- New Feature Highlights
- Miscellaneous (not discussed in other presentations)

Tivoli software

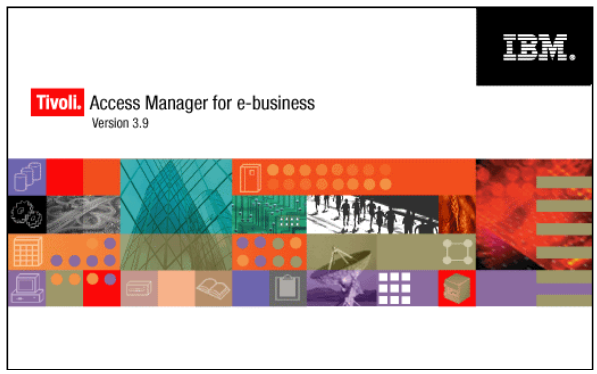
IBM

2


EMEA ATS PIC
Recent & Upcoming News
(and small amount of Marketing)
Tivoli software
IBM
3

Policy Director has New Name!

EMEA ATS PIC



~~IBM Tivoli Policy Director~~

IBM Tivoli Access Manager for e-business

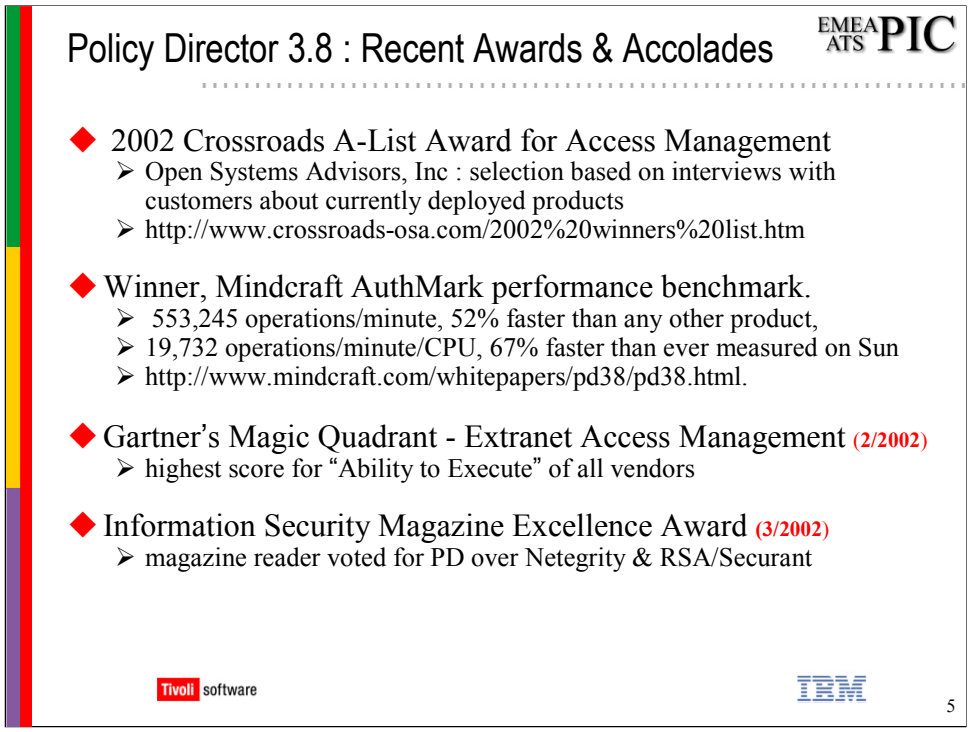
Tivoli software

IBM

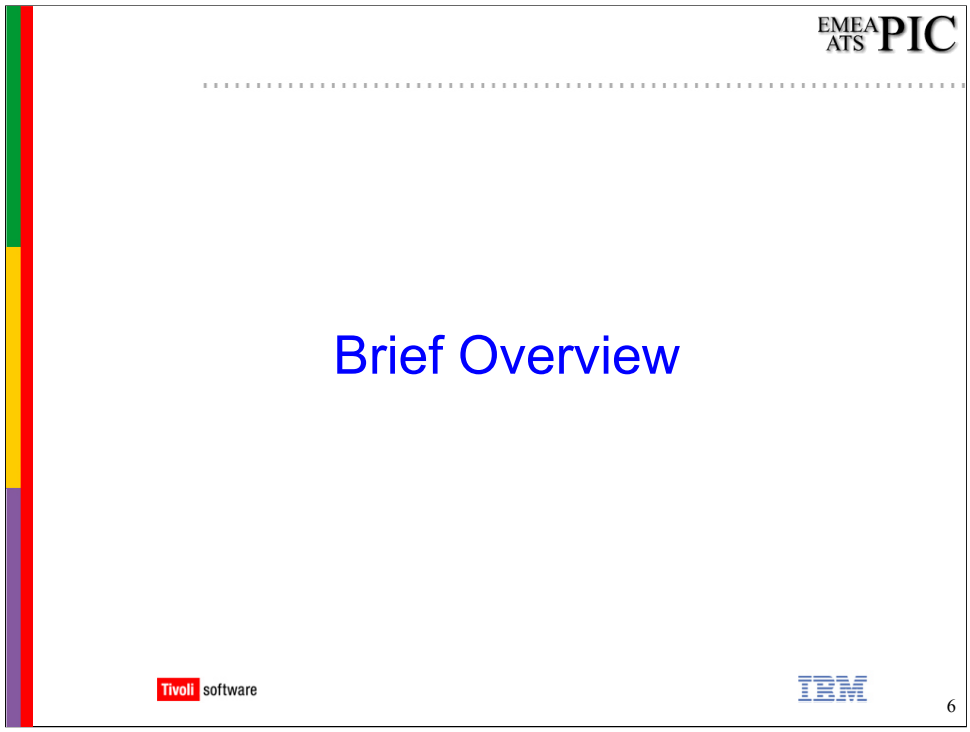
4

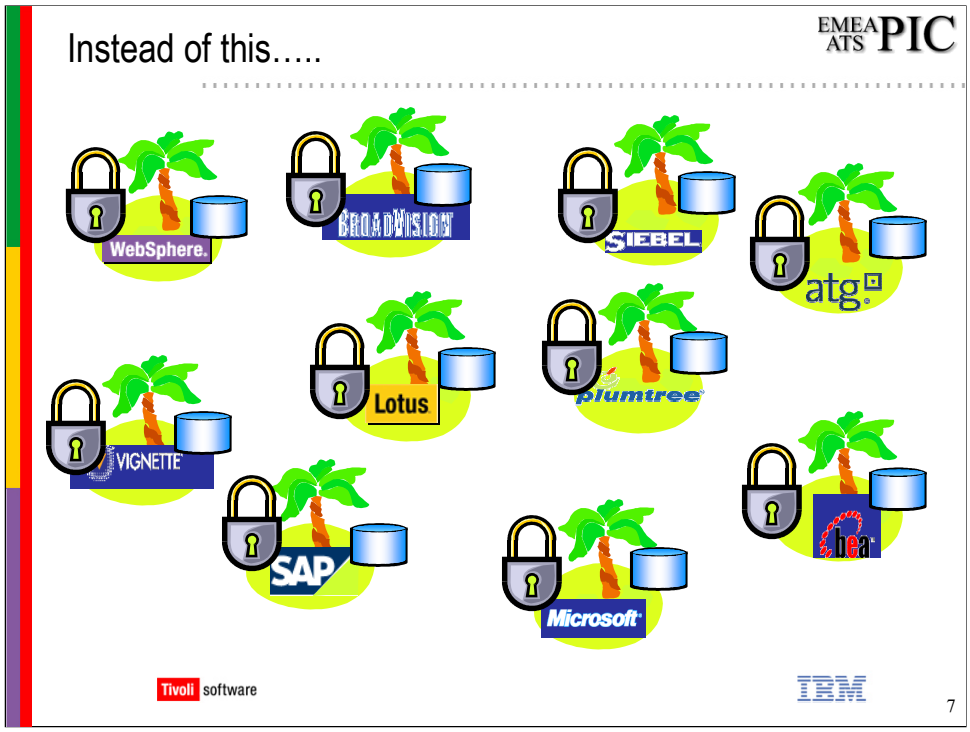
Some places in the product will still say “Policy Director” -> think “Access Manager”.

When you see “PD”, think “AM”

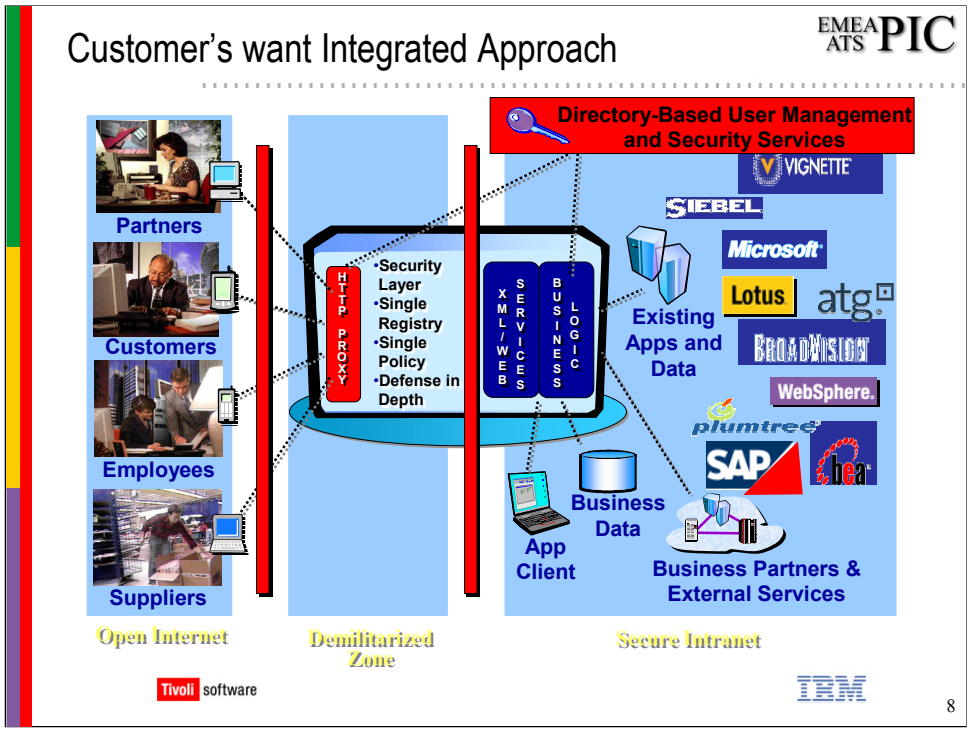


This is the only marketing you will find in all the workshop material. The recent news, however, is so good we just had to put some in.


EMEA ATS PIC
Brief Overview
Tivoli software
IBM
6



Each vendor has, over the years, provided their own vision of security. The result is that a large enterprise is populated with multiple 'islands of security' that are difficult (if not impossible) to manage with clear, simple policy that is necessary for effective security.

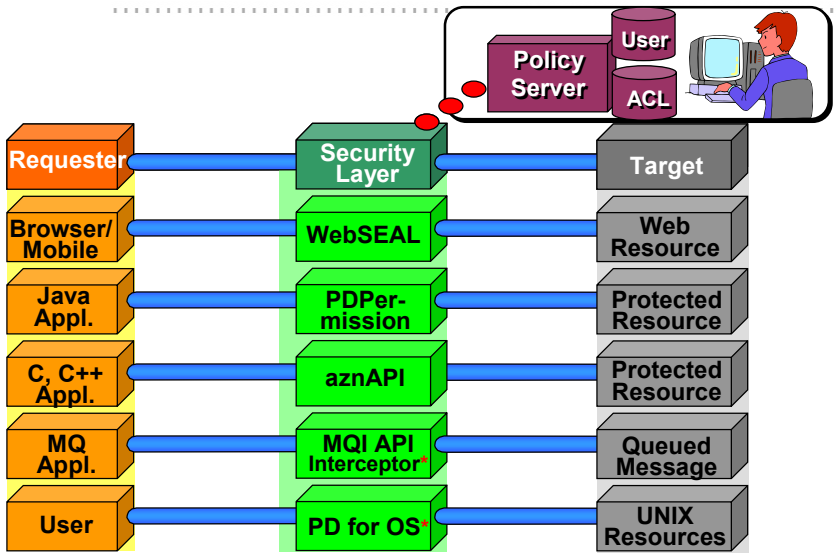


Access Manager provides the components and tools to define the security policy *within the infrastructure* of the enterprise. Minimizing configuration requirements and maximizing efficiency and security.

An excellent source for integration information is http://integration.santacruz.na.tivoli.com/. IBM internal network.

Security Policy in the Infrastructure….

EMEA ATS PIC

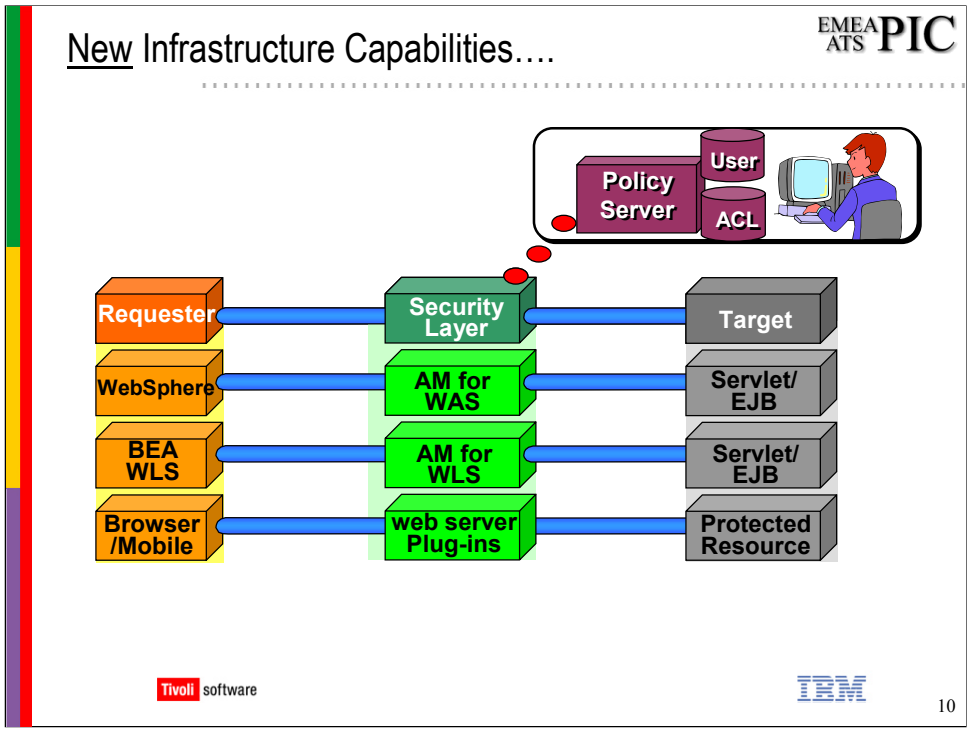


*Separately orderable product

Tivoli software

IBM

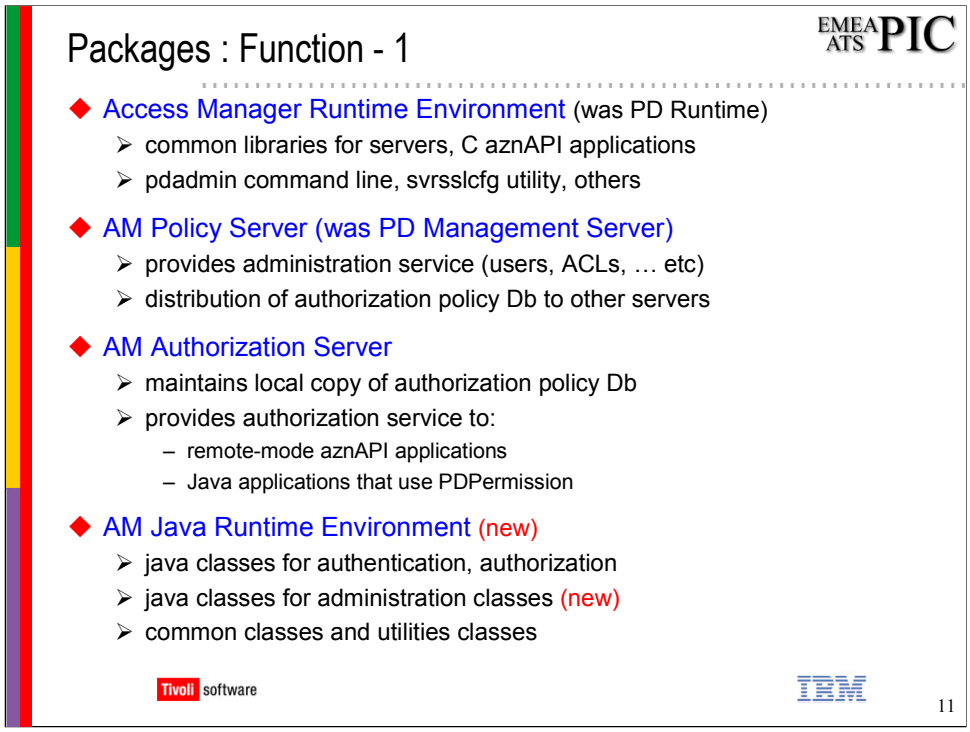
9



Policy Director 38. for Web Application Server 4.02 and Policy Director 3.8 for BEA WebLogic Server are available for web download to registered PD Customers.

The web server plug-ins are new to version 3.9

Access Manager 3.9 for WebSphere Application Server and AM 3.9 for WebLogic Server will have new features. These new features will be covered in the AM for Application Servers presentation.



The full name of each package is actually "IBM Tivoli Access Manager xxxxxx". For example,

- IBM Tivoli Access Manager Policy Server
- IBM Tivoli Access Manager Authorization Server
- etc

This slide lists some installable packages of Access Manager for e-business, and provides a high-level overview of the package. It does not attempt to provide a complete description of the function provided by that package.

Packages : Function - 2

EMEA ATS PIC

- AM Authorization ADK
  - libraries, header files for 'C' applications : aznAPI & Admin API
  - demo applications (java & 'C')
- AM Web Portal Manager
  - WebSphere application for AM Administration
- AM WebSEAL
  - extensive feature reverse-proxy web server for access management of web resources
- AM WebSEAL ADK
  - custom authentication library (CDAS)
  - cross domain name mapping CDMF (used only with ecSSO)
  - password strength library

Tivoli software IBM

12

The Authorization ADK provides demo applications for:

- •administration & authorization (java and 'C')
- •external authorization and admin service ('C' only)

This slide lists some installable packages of Access Manager for e-business, and provides a high-level overview of the package. It does not attempt to provide a complete description of the function provided by that package.

Packages : Function - 3

EMEA ATS PIC

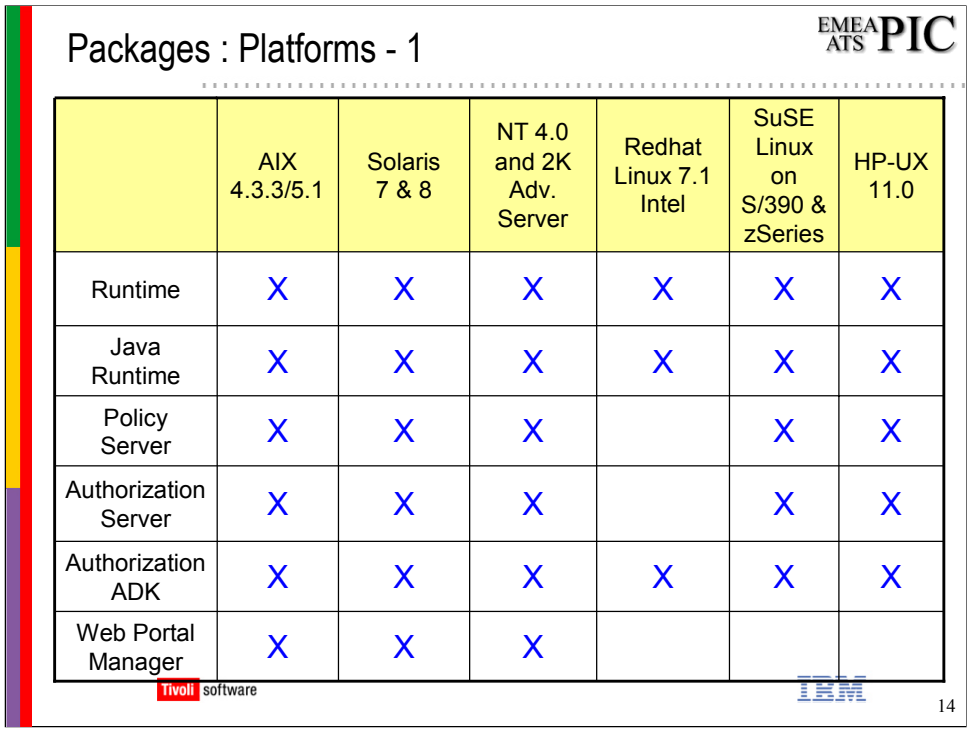
- AM for WebSphere Application Server (new platform/registry)
  - authorization service using AM Authorization Server
- AM for BEA WebLogic Server (new platform/registry)
  - authentication to AM User Registry
  - authorization via AM group membership
  - SSO with WebSEAL
- AM Plug-in for WebSphere Edge Server
  - authorization, authentication with local AM policy Db
  - custom authentication library (CDAS) (new)
- AM Plug-in for WebServers (new)
  - authorization, authentication with local AM policy Db
  - many, not all, features of WebSEAL

Tivoli software IBM

13

The 'new-ish' features are features that are included with AM 3.9, but are also recently available (via web download) features for Policy Director 3.8.

This slide lists some installable packages of Access Manager for e-business, and provides a very high overview of the package. It does not attempt to provide a complete description of the function provided by that package.



These Runtime, Java Runtime, Policy Server, Authorization Server and Authorization ADK are referred to collectively as “Access Manager Base”.

IBM SecureWay LDAP 3.2.2 is provided for all Access Manger Base platforms except HP-UX.

The precise platform requirement for Linux on S/390 & zSeries hardware is “SuSE Linux Enterprise Server 7 for S/390 and zSeries (2.4 Kernel based)”

Packages : Platforms - 2

EMEA ATS PIC

	AIX 4.3.3/5.1	Solaris 7 & 8	NT 4.0 Windows 2000 Adv. Server	Redhat Linux 7.1 Intel	SuSE Linux on S/390 & zSeries	HP-UX 11.0
WebSEAL	X	X	X		X	X
WebSEAL ADK	X	X	X		X	X
AM for WebSphere	X	X	X	X		X
AM for WebLogic Server	X	X	X	X		X
AM Plug-in for WAS Edge Svr.	X	X	2K Only[1]	X		
AM Plug-in for Web Servers	IBM HTTP Svr 1.3.19 on AIX 5	iPlanet 6 on Solaris-7[2]	IIS V5 on Win 2K Server			

Tivoli software

IBM

15

1) WebSphere Edge Server 4.02 does not support Win NT

2) iPlanet 6 on Solaris-8 is high priority.

Pre-requisites - 1

EMEA ATS PIC

- Runtime Environment
  - GSKit 5.0.4.67
  - LDAP 3.2.2 client (except for Active Directory)
- Java Runtime Environment
  - Java 1.3
- AM Policy & Authorization Servers
  - AM Runtime Environment
- AM Web Portal Manager
  - AM Runtime Environment
  - WebSphere 4.02
- AM Authorization & Administration applications
  - AM Java Runtime -- or –
  - Runtime Environment ('C' applications)

Tivoli software

IBM

16

Pre-requisites - 2

EMEA ATS PIC

- WebSEAL
  - AM Runtime Environment
- AM for WebSphere Application Server
  - AM Java Runtime Environment
  - WebSphere 4.02
- AM for BEA WebLogic Server 6.1
  - AM Runtime Environment w/ LDAP Client
  - AM Java Runtime Environment
- AM Plug-in for WebSphere Edge Server
  - AM Runtime Environment
  - WS Edge Server 2.0 plus ptf-1 (2.01)
- AM Web Server Plug-ins
  - AM Runtime Environment

Tivoli software

IBM

17

Directories

EMEA ATS PIC

- IBM SecureWay Directory v3.2.2
  - LDAP Server can be 3.2.1 or 3.2.2
    - AM always uses IBM SW 3.2.2 client
  - LDAP 3.2.2 packaged with AM
    - Includes DB2 Personal Edition v7.2
    - AIX 4.3.3/5.1, Solaris 7/8, Win NT/2K, Redhat Linux 7.1
- iPlanet Directory Server 5.0
  - Server available on all AM platforms
    - Access Manager uses IBM SW LDAP 3.2.2 client
  - AM packages available on all platforms (I.e, no client pre-req problem)
- Lotus Domino Server 5.0.4 (new)
  - Server available on all AM platforms
    - Access Manager uses both Notes & SW LDAP 3.2.2 client
  - AM packages available only on Windows
- Active Directory (new)
  - Windows 2000 Advanced Server
    - Access Manager uses ADSI client
  - AM packages available only on Windows 2000

Tivoli software

IBM

18


EMEA ATS PIC
New Feature Highlights
Tivoli software
IBM
19

New Directory : MS Active Directory

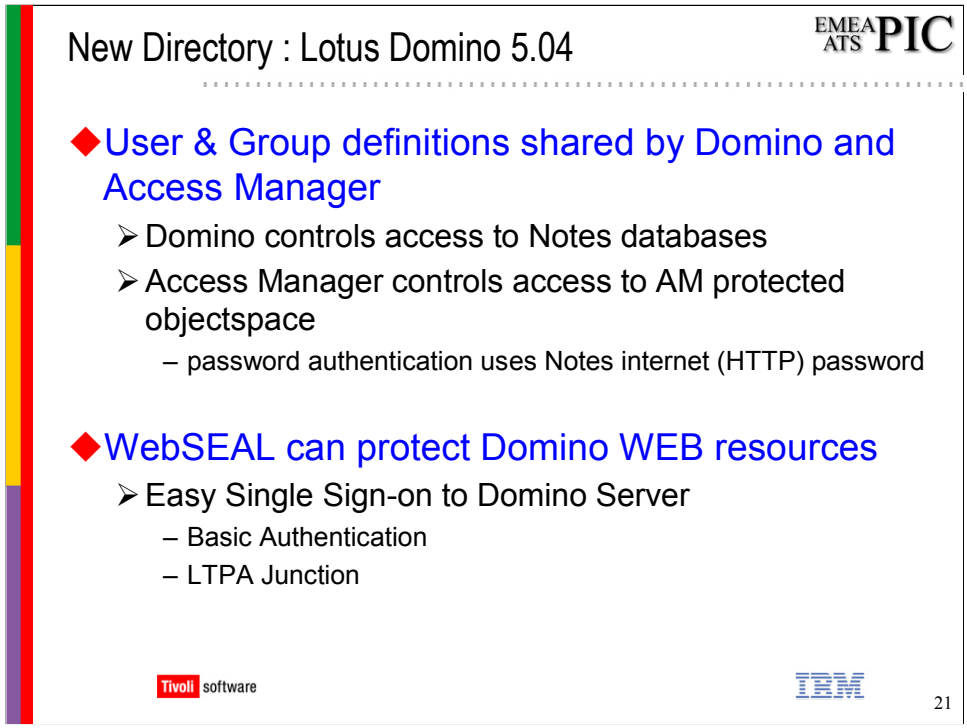
EMEA ATS PIC

- Two modes of configuration:
  - **single-domain** : all users/groups in single AD Domain
  - **multi-domain** (single forest)
    - users can be defined in any domain
    - group & users must be in the **same domain** (Universal group not supported in this release)
    - a Global Catalog **must** be available in forest
- Failover Support
  - **single-domain** – fail-over support to multiple domain controllers
  - **multi-domain** :
    - failover support to multiple domain controllers in forest root only
    - when domain controller in non-root domain fails, other domains continue to operate
  - no “prefer replica” support – failover is to any available domain controller

Tivoli software

IBM

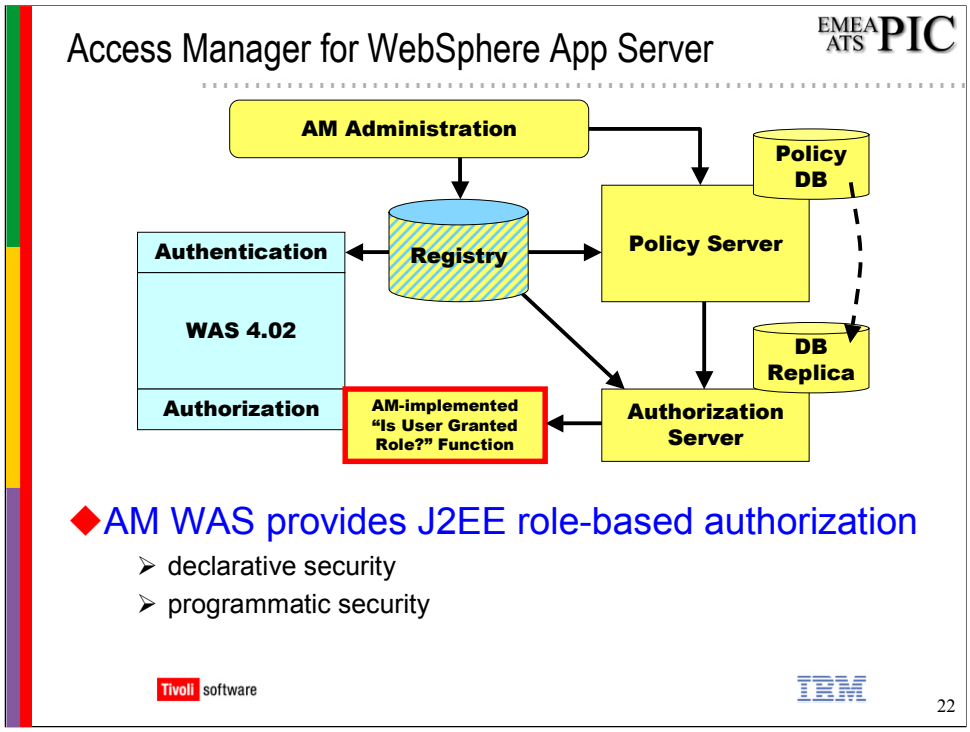
20



Using Lotus Domino as the Policy Director user registry means using the Domino Notes Address Book (NAB) as the repository of user information rather than using LDAP.

The user definitions in the NAB are shared between Policy Director and Domino. This means that there are no user synchronisation problems for applications using user definitions in the NAB. Any user created by Policy Director (or created by Domino and imported into Policy Director) can access both Domino and Policy Director resources using the same identity.

The sharing of the user identity information (namely the users shortname and Internet password) means that achieving single sign-on is much simpler.



TAME 3.9 provides:

-an integration module that uses AM for WAS authorization requirements

-a migration utility for use with WAS applications

AM Administration applies ACLs to Role objects defined in AM protected object space. The AM ACL provides Role->Principal (user & group) mapping.

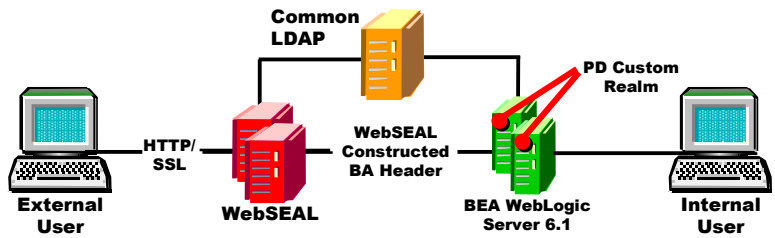
The **migration utility** examines the J2EE application deployment descriptor for:

•Declared Roles → used to create objects in AM protected object space

•WebSphere .xmi files → used to create ACLs for that role

Access Manager for BEA WebLogic Server

EMEA ATS PIC



- Single Signon with WebSEAL
- Provides use of Access Manager User Registry for WLS (significant cost savings)
- User/Group Administration from WLS Console, or AM Administration
- User-to-group assignments control J2EE authorization decision of WLS

Tivoli software

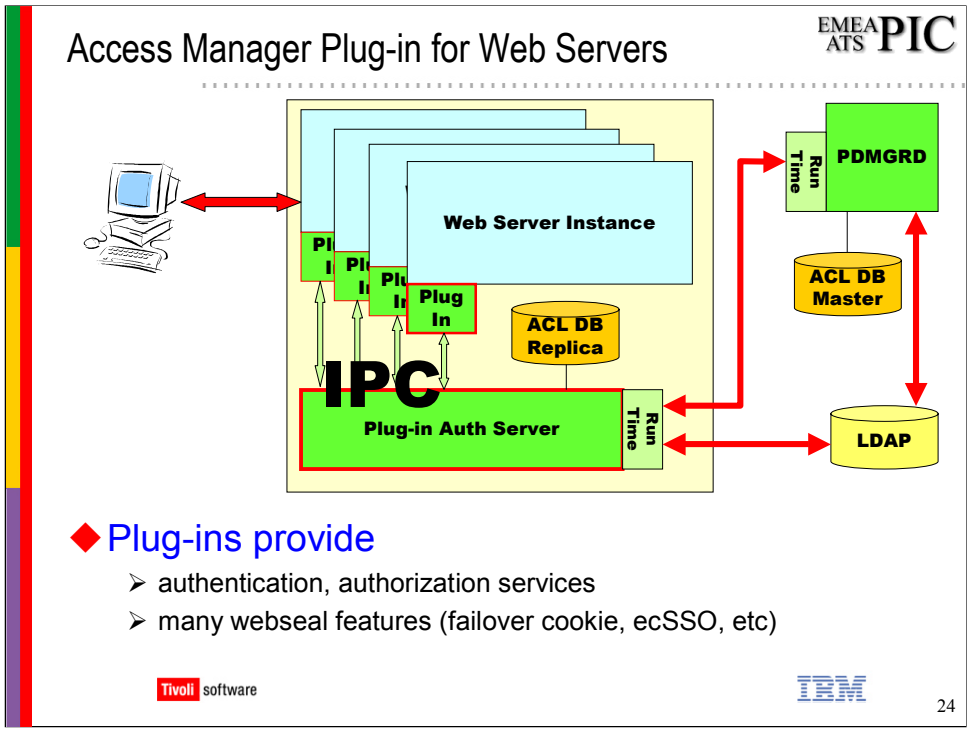
IBM

23

TAME 3.9 provides an implementation of the BEA WLS *Custom Realm*.

The Custom Realm provides these services to BEA WLS 6.1:

- •User management (create, list, delete)
- •User authentication - UserId/Password
- •Group management
  - •add/remove user from group
  - •list user
  - •answer group membership for user → used in authorization decision



The Access Manager Plug-in for Web Servers provides these benefits:

- allows use of preferred web server in DMZ
- eliminates the need for changes to edge network topology
- provides several of features provided by WebSEAL

For optimum security, the the AM Plug-ins should only be used when either:

- the web server is configured as a reverse-proxy to other servers in the secure network
- the web server is only hosting the presentation tier of J2EE applications where the business logic executes on an application server in the secure network.

Without one of these conditions, the benefits of a “security in depth” architecture with ‘Internet | DMZ | secure-network’ topology are compromised due to the direct access of unauthenticated users to business logic.

New Features : WebSEAL

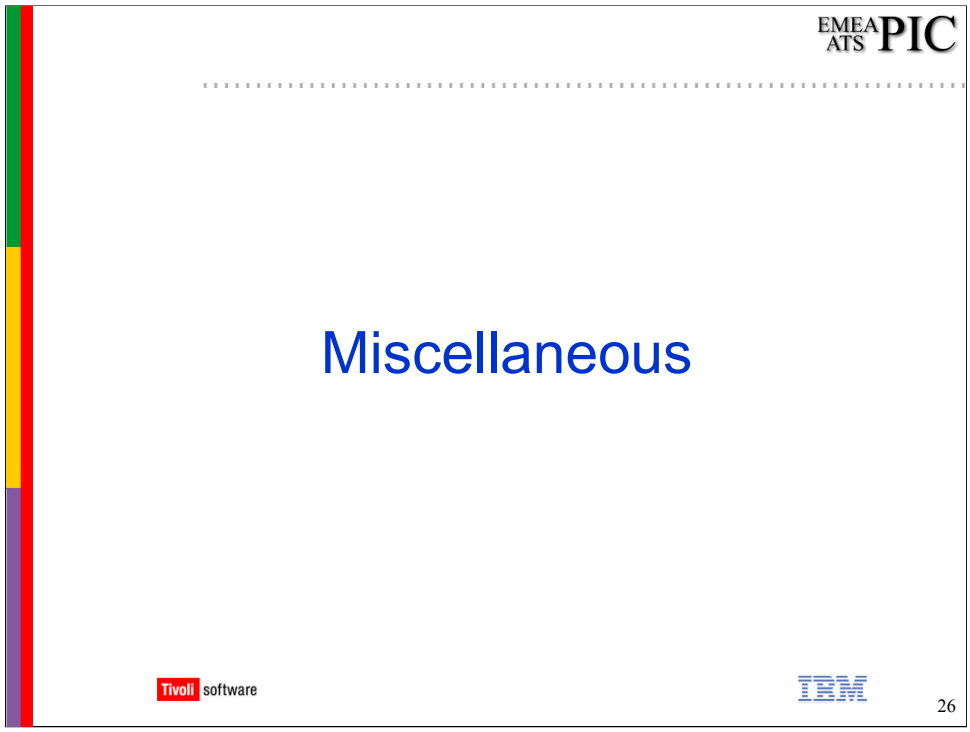
EMEA ATS PIC

- Multiple WebSEAL on single machine
  - effectively “hardware-based” virtual hosting
- HTTP 1.1 support to back-end web servers
- HTTP Request Cache
  - solution for ‘Lost POST data’ problem with form-login
    - initial authentication or re-authentication
- Forced re-Authentication via access policy
- Force User Logout
- Switch User Capability
- Thread management by back-end junction
- Hardware accelerator support
  - nCipher nForce 300 on Windows & Solaris

Tivoli software

IBM

25


EMEA ATS PIC
Miscellaneous
Tivoli software
IBM
26

New Features : Web Portal Manager

EMEA ATS PIC

- Support for AIX and Solaris
- Signon via Basic Authentication header
  - Allows SSO from WebSEAL using GSO or other
    - other '-b' or '-B' options possible for 'same access' groups
- Usability Improvements
  - Objectspace 'Explorer'
  - "Pop-up list" for by ACL/POP attach
- New function
  - Create for Object & Objectspace
  - Create for Action & Action Group
- Customisation
  - Replace login pages with Customer design

Tivoli software

IBM

27

AM Java Runtime

EMEA ATS PIC

- Manual configuration only
  - use "<AM-Install>/sbin/pdjrtecfg" utility
- Contains all classes for AM Java applications
  - Authentication & Authorization
    - PDPrincipal & PDPermission
  - Administration API
    - subset of 'C' Administration API
- Easier SvrSslCfg operation to establish JVM trust
  - Specify only user 'shortname'
    - User created and added to 'remote-acl-users' group
    - only syntax supported for Active Directory and Domino
- Access to aznAPI Entitlements Service
- Jlog used for common logging format/configuration
  - configured via 'pdjrtecfg' utility

Tivoli software

IBM

28

AM 3.9 WES Plug-in Enhancements

EMEA ATS PIC

- Additional platforms
  - Solaris 7 & 8 and AIX 5.1
- Cross Domain Authentication Service interface (CDAS)
  - Allows custom authentication service
  - Similar to WebSEAL CDAS interface
  - Allows customization of
    - User/Password
    - Certificate
    - "Accept SSO" – CDAS receives request URL & Headers
- Store POST data of http request during authentication
- Performance & Documentation Enhancements

Tivoli software IBM

29

Upgrade/Migration

EMEA ATS PIC

- Upgrade Install (native install only)
  - Install 3.9 on top of current installation
    - Current installation must be 3.7 or 3.8
  - Data migration required for 3.7
    - No changes in data format between 3.8 & 3.9
- Installations prior to PD 3.7 must first be migrated to PD 3.7.1
- Migration Tool also supports data backup/restore

Tivoli software

IBM

30