Access & Security Management
Technical Introduction

Chris Van Den Abbeele
Technology Specialist IDM, Novell

Emmanuel Limage
Consultant, OPNS

September, 2006
Agenda

- Access Manager In General
- Access Manager Components
- Federation (SAML / Liberty)
- NAM component: Identity Provider (IdP)
- NAM component: Access Gateway (LAG/NAG)
- NAM component: SSL-VPN
- NAM component: JAVA/J2EE Agents
- NAM component: Secure Logging
- NAM component: 5 types of Policies
- SSL-ization
- Mapping NAM to iChain
Functions/aspects of an Access Management Solution

- reverse proxy
- central authentication point
- authentication mechanisms (passw, token, certificate,...)
- multi-homing (URL recombination)
- abstraction (URL / IPaddress)
- acceleration (caching)
- URL based security (public, restricted, secure)
- user store
- Role Based Access Control (RBAC)
- authorizations store (which Roles grants which Access)
- Single Sign On
- management console(-s)
- Federation
- SSL-VPN
Novell Access Manager

- Next Generation Access Management Solution
  - 1. Secures HTTP applications via **Access Gateway**
  - 2. Secures non-HTTP applications via **SSLVPN**
  - 3. EJB and Servlet fine grained access control via **Java Agents**
  - 4. Extensible **Policy Engine providing Role Based Access Control**
  - 5. Identity Federation (**SAML and Liberty Alliance**)  
    - No need to modify web applications to take advantage of new Federated Identity standards.
Looking back at iChain
iChain Architecture and components

- iChain Proxy Server
- iChain Authorization Server
- Console One / Proxy Console
Limitations of iChain

• A pure Reverse Proxy becomes “blind” when the URL stops changing (after an EJB / Servlet is launched)

• Administration
  - Need to connect to each proxy to configure it (often its the same accelerator configuration)

• SAML and Liberty Alliance
  - Supports SAML 1.0 only
  - has no support for Liberty Alliance

• Access Control of non-HTTP applications
  - Support for Citrix ICA clients only
Access Manager: Architecture and Components

- Access Gateway
- Identity Server
- Device Manager
- Java Agents
- SSL-VPN

![Diagram showing the architecture and components of Access Manager.](attachment:image.png)
Access Manager : access-flow

1. The user requests access to a resource protected by the Access Gateway.
2. The Access Gateway redirects the user to the Identity Server, which prompts the user for a username and password.
3. The Identity Server verifies the username and password against an LDAP directory (eDirectory, Active Directory, or Sun ONE).
4. The Identity Server returns an authentication success to the browser and the browser forwards the resource request to the Access Gateway.
5. The Access Gateway verifies that the user is authenticated and retrieves the user’s credentials from the Identity Server.
6. The Access Gateway uses an identity injection policy to insert the basic authentication credentials in the HTTP header of the request and sends it to the Web server.
7. The Web server grants access and sends the requested page to the user.
Novell Access Manager Components (what comes in the box)

Product Components
- **Identity Server** central server that keeps track of who has access to what – all Novell access manager gateways point to it to verify users and access
- **Access Gateway** as the access control point to enforce security for web-based applications and systems
- **SLLVPN** – Secure channel to non-browser-based applications (mainframes for instance) can share Single-Sign-on with web-based applications.
- **Java agents** so the identity server, access gateway and target systems (web servers) can talk to one another
- **Centralized Management interface** (iManager)

Benefits
- Precise control over digital assets
- Unmatched security that safeguards network data
- Improved end-user experience
- Accelerated return on e-business-application investments
- Reduced administration and security costs
Administration
(Device Manager, this is not a full iManager)
What is account federation?
(SAML and Liberty)
Federation Defined

• What is Federation?
  - A Federation is a group of two or more trusted business partners with business and technical agreements, which allow a user from one federation partner, to seamlessly access resources from another partner in a secure and trustworthy manner.
  - It's the evolution of Identity & Access Management.
Federation Standards

- SAML 1.1
- Liberty Alliance
- (WS-*)
- SAML 2.0
- A close history, together
Security Assertion Markup Language (SAML)

- Developed by OASIS at the Security Services TC (SSTC)

- 1. Defines *assertions* which carry statements

- 2. Provides a protocol for disseminating assertions among *authorities* and *relying parties*

- 3. A set of profiles to provide Web-based simplified sign-on
SAML & Liberty

- Liberty added profiles to SAML 1
- Liberty is user-centric: The user decides if and what parts of his identity he federates
- Now they are closely together
Liberty Alliance Basic Federation

Users decide who they want to federate their identity with

- Federation is actually the linking of two accounts using a unique pseudonym. The user account must already exist in both locations.

1. User authenticates to Identity Provider
2. User authenticates to a Service Provider, which recognizes he has a trusted Liberty authentication
3. User is asked if he wants to Federate his Identity
4. A unique pseudonym is created and associated with the identity at both the Liberty and Service Provider
Liberty Alliance Framework

- Specification has evolved into a secure method of federating users and exchanging identity

Liberty Identity Federation Framework (ID-FF)

Enables identity federation and management through features such as: identity/account linkage, simplified sign on, and simple session management

Liberty Identity Services Interface Specifications (ID-SIS)

Enables inter-operable identity services such as personal identity profile service, alert service, calendar service, wallet service, contacts service, geo-location service, presence service and so on

Liberty Identity Web Services Framework (ID-WSF)

Provides the framework for building inter-operable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles

Liberty specifications build on existing standards
(SAML, SOAP, WSS, XML, etc...)
SAML federation

- common with Liberty:
  - The account must exist at both sides it does not have to be the same account name, but it must have a common identifier

- difference with Liberty:
  - SAML is a better fit for the business model where:
    - not the user federates his accounts
    - but an admin has a pre-defined setup for federation

- Federated Provisioning (NAM silver bullet)
  - Federated Provisioning automatically creates the user account on the consumer site, following pre-defined rules.
  - also called: "just in time provisioning"
Defining Identity Sharing Policies

To define Identity Profile Sharing, the user first selects the required Service Provider.

The Novell® Access Manager user interface presents the profiles and allows the user to set a policy on the entire profile or to click into the profile to specify policy on specific pieces of their Identity.
Novell Identity Server
Identity Server

- Role Distribution to other components
Identity Server

- Novell Access Manager Identity Server
  - Liberty Alliance v1.2 Identity Provider
  - ID:WSF (Identity Exchange)
  - SAML 1.1 and 2.0 Consumer / Provider
  - Federated Provisioning (*competitive advantage*)
  - Authenticates Users (direct or via federation)
  - Role Distribution

- Supported Identity Stores
  - eDirectory
  - Active Directory
  - Sun One
Identity Server

- **Authentication Methods**
  - UserID and Password (LDAP validation)
    - Support for multiple LDAP source
  - X.509 (CRL and OCSP supported)
  - Token Authentication (via RADIUS)
  - Custom
    - build-yourself using NMAS API
    - Third Party Authentication Vendors

- **Supported Platforms**
  - SUSE Linux Enterprise Server
  - Windows 2003 (in NAM3sp1)
Novell Access Gateway
Access Gateway

- Novell Access Manager Access Gateway
  - Secures HTTP Applications
  - Provides Liberty SP enabled SSO
  - Supports Form Fill & Header Based SSO to back-end applications
    - both Policy based
  - Provides Identity Injection (formerly OLAC)
    - policy based
  - Secure Exchange (SSLizer)
  - Multi-homing (domain- and path-based)

- Supported Platforms
  - NetWare 6.5 and Linux SLES 9 (both appliance type install)
Access Gateway

- Management
  - Centrally managed from iManager
    - One place to configure and view all Access Gateways

- Provides Grouping Capability
  - One change affects multiple Access Gateways
Access Gateway Configuration

Novell Device Manager

User: Admin

Reverse Proxy Host: AGTest2 - Test - Host

Public Host DNS Name: www.novell.com
Description:
Cookie Broker: Host

Enable Browser Caching
HTTP Options

Web Servers

Web Server Options
Web Server List
Delete
Web Server

Path-based Multi-homing

Path-based Multi-homing List
Delete
Multi-homed Paths
Web Server Addresses

Security Settings

Authentication Options
Protected Resources

OK Cancel
Protected Resource Configuration
Access Gateway

- Authorization *Policies* determine Roles
  - Roles determine Access (RBAC)
  - Supports Custom Authorization Decisions (call-out to external process)
- Policy Management
  - All policies administered from iManager
SSL is enabled as an option on the Web server accelerator configuration dialog box.

SSL is an ON/OFF option for each accelerator.
SSLVPN
SSLVPN

- Linux-based SSLVPN Service
  - Provides secure access to non-HTTP applications
  - SSLVPN device is accelerated by Access Gateway
    - User must authenticate before a session can be established
  - Active-X and Java Applet client (delivered on-the-fly)
  - Client Integrity Checking
  - Traffic **Policies** determine what back-end applications can be accessed
Tested Applications

- FTP
- Telnet
- SSH
- Citrix ICA Client
- MS Terminal Client Service
- Outlook Client
- Remote Desktop
- GroupWise 6.5 mail client

NOTE: Currently SSL VPN does not support any UDP applications.
SSLVPN Scenario 1

• SSLVPN on Linux Access Gateway
SSLVPN Scenario 2

- SSLVPN on Separate Server
SSLVPN

- Client Integrity Checking
  - Search for Firewall
    - Norton, McAfee, Zone Alarm
    - Custom (search for specific files)
  - Search for Virus Scanner
    - Norton, McAfee
    - Custom (search for specific files)
  - Corporate Required Software
    - Searches for specific files
SSLVPN

· Traffic *Policy* Configuration
  - Access to specified IP / DNS address
  - Access to specified port numbers
  - Access based on User Identity (attributes)
  - Access based on status of client integrity check
  - Access based on authentication method used
Configuring Browsers for SSLVPN

- Mozilla Firefox
  - JRE 1.4 or higher installed
  - **Java** enabled in Firefox
  - Firefox cache is clean

- Internet Explorer
  - **ActiveX** and Scripting enabled
  - Add SSLVPN URL to trusted sites
  - Clean Cache
Accessing the SSLVPN

- Access SSLVPN URL
- Specify user and password
- Click Yes to accept and download the SSLVPN client
Java Agents
Secure Access to Java Applications

1. User accesses JBOSS application either directly (1a) or via a protected resource on the Access Gateway (1b)

2. User is redirected to the Identity Server and is presented with a login dialog requesting their username and password, which is validated against the Identity Store

3. The Identity Server builds the user's role(s) and redirects the user back to the JBOSS application (direct or via Access Gateway)

4. The JBOSS application server evaluates the roles and grants or denies access to the request
Java/J2EE Agents

- Java Agents Provide
  - SSO to Java Application
  - Fine-grained Access Control to EJB and Servlets
    > impossible with iChain as the URL stops changing after the EJB/Servlet is launched
- Supported Application Servers (JAAS/JACC)
  - Jboss 4.0.3 SP1
  - IBM WebSphere
  - BEA WebLogic
- Supported Platforms
  > Linux and Windows 2003
  > Java Authorization Contract for Containers is a set of security contracts defined for the EJB and Web containers. ...
  > JAAS: Java Authentication and Authorization Service is a package that enables services to authenticate and enforce access controls upon users.
Enterprise Archive

Enterprise Archive (.ear)
application.xml

web archive (.war)
web.xml

EJB archive (.jar)
ejb-jar.xml

resource archive (.rar)
ra.xml
Java Application Requirements

• Need to know the Roles defined in the Application
  - Defined in application.xml, web.xml, and/or ejb-jar.xml

• Need to alter web.xml
  - Login Servlet – specify the AMgr login class
  - Logout Servlet – specify the AMgr logout class
Application.xml (part of the ear)

- <application>
  <display-name>PayrollApp</display-name>
  <module id="PayrollEJB.iml">
    <ejb>PayrollEJB.jar</ejb>
  </module>
  <module id="PayrollWeb.iml">
    <web>
      <web-uri>PayrollWeb.war</web-uri>
      <context-root>/payroll</context-root>
    </web>
  </module>
  <security-role>
    <role-name>Manager</role-name>
  </security-role>
  <security-role>
    <role-name>Employee</role-name>
  </security-role>
</application>
web.xml Login Alterations

- `<servlet>
  <servlet-name>LoginServlet</servlet-name>
  <servlet-class>
    com.novell.nids.agent.auth.LoginServlet
  </servlet-class>
</servlet>

- `<servlet-mapping>
  <servlet-name>LoginServlet</servlet-name>
  <url-pattern>/login</url-pattern>
</servlet-mapping>`
web.xml Logout Alterations

- `<servlet>
  <servlet-name>LogoutServlet</servlet-name>
  <servlet-class>
    com.novell.nids.agent.auth.LogoutServlet
  </servlet-class>
  <init-param>
    <param-name>postLogoutURL</param-name>
    <param-value>/</param-value>
  </init-param>
  <init-param>
    <param-name>invalidateHttpSession</param-name>
    <param-value>true</param-value>
  </init-param>
</servlet>

<servlet-mapping>
  <servlet-name>LogoutServlet</servlet-name>
  <url-pattern>/logout</url-pattern>
</servlet-mapping>
Secure Logging
Novell Access Manager Logging
Novell Audit Support

- Access Manager includes a fully licensed version of Novell Audit 2.0.2 server and platform agent
  - limited for use with Access Manager
- Access Manager can be configured to use the internal Novell Audit server or another external Novell Audit server (only one at a time).
Novell Access Manager Logging Alerts - Novell Audit Notifications

- Access Manager leverages Novell Audit notifications for sending alerts
- Supported Novell Audit output driver channels for alerts:
  - SYSLOG
  - SMTP (email)
  - SNMP (single OID)
- Configure Novell Audit notifications to translate individual events into alerts
  - No extra Access Manager configuration required (other than enabling Novell Audit events)
Access Manager Policies
Access Manager Policies

- Rule-based logic to maintain order, security, and consistency
- Rule contains condition(s) and action(s)
- If the condition list is met, the actions are performed
- Policy Types
  - Access Gateway: Identity Injection
  - Access Gateway: Form Fill
  - Identity Server: Roles
  - Access Gateway: Authorization
  - Java Agent: EJB Authorization
  - Java Agent: Web Authorization
Identity Injection Policies

- Retrieve data from LDAP and use it for access control
- Formerly known as OLAC
- [Protected resource]>Identity Injection
- Build rule to insert credentials (uid/pwd) into Authentication Header
Identity Injection Policies

![Image of Identity Injection Policies interface](https://idpa.am3.com:8443 - Rule - Mozilla Firefox)

- **Edit Policy: II_of_Credentials - Rule 1**
- **Description:**
- **Priority:** 1

**Actions**

- **Do Insert Into Authentication Header:** User Name: [Credential Profile] : [Credential]
- **Password:** [Credential Profile] : [Credential]

*Changes made on this panel must be applied from the Policies Panel.*

[OK] [Cancel]
Role-based Policies

· Evaluates rules for establishing the roles for an authenticated users
· Uses these roles in other policies
Role-based Policies

Edit Policy: Sales_Role - Rule 1

Description:
Priority: 1

Conditions
Condition structure: AND Conditions, OR group:
If

Condition Group 1
Liberty User Profile: Internal Job Title
Comparison: String Equals
Flags: Case Sensitive
Value: Data Entry Field: Sales

Actions
Add Role: sales_role

Changes made on this panel must be applied from the Policies Panel.

OK Cancel
Authorization Policies

- Use rules to control access to protected resources
- Often based on roles or identity injection
- Tied to a protected resource
Authorization Policies

https://idpa.am3.com:8443 - Rule - Mozilla Firefox

Edit Policy: allow_sales - Rule 1

Description:
Priority: 1

Conditions
Condition structure: AND Conditions, OR group

If Not

Condition Group 1
New

If Roles for Current User
Comparison: String
Contains Substring
Flags: Case Sensitive
Value: Data Entry Field: sales_role

Actions
Do Deny: Message: Sorry, you must work

Changes made on this panel must be applied from the Policies Panel.

OK Cancel

Done idpa.am3.com:8443 Adblock
Form Fill Policies

- No XML
- GUI Policy Editor
Policy Editor

Fill Options

<table>
<thead>
<tr>
<th>Input Field Name</th>
<th>Input Field Type</th>
<th>Input Field Value</th>
<th>Data Conversion</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Text</td>
<td>Credential Profile</td>
<td>LDAP Credentials:LDAP User Name</td>
</tr>
</tbody>
</table>

Post Options

- Auto Submit
  - Debug Mode
  - Mask Data
- Insert Text in Post Header
  - Post Header Text...
- Enable JavaScript Handling
  - Functions to Keep...
  - Statements to Execute on Post...

Error Handling

Redirect to URL: ____________________________
Mapping Access Manager to iChain
Map the functions to the components

- **Authentication**
- **Identity Store**
- **embedded eDir**
  what is it used for? where is it?
- **product configuration store**
- **Administrative Interface(s)**
- **where do we run the SSLVPN component?**
- **do this for iChain and for Access Manager and identify at least 3 differences**

- **Access Gateway (Linux or Netware based version)**
- **Identity Server**
- **embedded eDir**
Clustering
High Availability
(in iChain, using the iChain session broker)

• iChain
  - what components need to be doubled?
  - what's the use of the session broker?

• Access Manager
  - what components need to be doubled?
High Availability (in iChain, using the iChain session broker)

what is the need for a session broker?
High Availability

- Which components need to be highly available?
Clustering Access Manager

- Identity Server
  - Scalability
- Access Gateway
  - Scalability
- Admin Server
  - Fail Over
Clustering Access Manager

1. User accesses URL
2. L4 directs user request to one of the available Identity Servers in cluster. If an Identity Server is unavailable the L4 will direct the request to another Identity Server.
3. L4 directs user request to one of the Access Gateways in the cluster. If an Access Gateway is unavailable the L4 will direct the request to another Access Gateway.
Identity Server Clustering

- Needs “sticky bit” enabled switch
- Session remains on same IDP server
- If that IDP fails, services remain up, but user should re-authenticate to other IDP
Configuring Identity Server Cluster

- Assign all of the servers to the same configuration.
Access Gateway Groups

- Group can't contain a mix of Netware and Linux
- Specify Primary Server
  - Settings pushed to other servers, but only initially
- From there settings managed from Admin Console
  - Some general for the Group
  - Some server-specific
- Session information is shared among the Access Gateway Group-members
Groups are a Cluster of A/G
Creating a Group

- Under the Group Tab Click “New”
Questions? Answers...
Thank You for your attention
Next Session after the break

• In this Room B: APPLICATION FIREWALL

• In the Room A: MOBILE MAIL