Novell® Access Manager
Product Overview

Kiran Mova
Agenda

Introduction

Architecture

IDP
AG
SSL VPN
Administration Console

How it works?

Web SSO
Federation SSO
Protect HTTP Resources
Protect non-HTTP Resources
Introduction

Access Manager is a set of components that help to:

- Provide Web and Federated SSO
- Protect HTTP/Non-HTTP enterprise servers
- Provide SSO to Legacy Web Servers

Also allows customers to extend:

- Authentication Mechanisms using Authentication SDK
- Authentication against Custom User stores using LDAP Server Plugin
- Policy Engine using Policy Extension API
Sample NAM Deployment

InnerWeb

Access Gateway (innerweb.novell.com)

  VersionOne (v1.innerweb.novell.com)

  Employee Self Service (psselfservice.innerweb.novell.com)

Identity Provider (login.innerweb.novell.com)

SSLVPN (sslvpn.innerweb.novell.com)
Admin Console – Key Features

Administration Console
Configure Components
Monitor Health and Statistics of Individual Components
Policy Administration
Certificate Management
Delegated Administration
Persistent configuration store
Granular Auditing (embedded NSure Audit Server)
Architecture – AC

Federated Identity Providers

Load Balancer

Authenticate

User

NAM

Device Manager
(iManager/Tomcat)

Config, Policy, Certificate Store

eDirectory

Clustering (eDirectory Replica)

Web UI (HTTPS)

Administrator

User Directory
(LDAP)

Authentication Servers
(RADIUS, etc.)

Mission Critical and Enterprise Data Systems.
HTTP and non-HTTP

Web UI

Certificate Store

JCC

Config, Policy (LDAPS)

Cert Configure (LDAPS)

Alerts
(HTTPS)

Configuration/Commands (HTTPS)

Audit (TCP)

Audit Cache

Identity Provider

Access Gateway

SSL VPN

Authentication Servers

Access Gateway

Load Balancer

Authenticate

User

Federated Identity Providers
Identity Provider – Key Features

Identity Provider (IdP)
- Authentication (includes x509, RADIUS..)
- Federated Authentication (SAML/ADFS)
- Associate Roles and Attributes with authenticated user
- Capable of authenticating against multiple User ID stores like eDirectory, Active Directory Sun One etc.,
- Extensible Authentication and Policy framework

SP (Service Provider) Agent
- Shared Component
- Redirects all authentication requests to IdP
- Maintains a cache of user data fetched from IdP
- Evaluates Policies by requesting additional data from IdP.
Access Gateway – Key Features

Access Gateway (AG)

Authentication (via Identity Server)
Authorization
Single sign-on to Legacy Web Servers (form-fill, identity injection)
Identity injection (personalization)
Secure exchange (SSLizer)
Multi Homing
Load Balancing
URL Normalization/ Rewriting
Caching
Policy Extensions API
Architecture - AG

Federated Identity Providers

SAML 2.0, SAML 1.x, Liberty, WS Fed (HTTPS)

Access Gateway

Liberty and Attribute Service (HTTPS)

Identity Provider

Audit (TCP)

Alerts (HTTPS)

Configuration (HTTPS)

NAM

Load Balancer

Clustering (JGROUPS)

Authenticate

Apache Instance

Audit Agent

JCC

RMI

HTTP (S)

Audit Agent

Gateway Manager

Session Cache

Active MQ

Connection (HTTPS)

Alerts (HTTPS)

Configuration, Policy (LDAPS)

Configuration, Policy (HTTPS)

SP Agent

SP Agent

JCC

RMI

HTTP (S)

Policy Extension API

Authentication Servers (RADIUS, etc.,)

User Directory (LDAP)

Mission Critical and Enterprise Data Systems. HTTP and non-HTTP

SSLS VPN

User

Clustering (JGROUPS)

HTTP(S)

SP Agent

Agent + Authentication

Servers

HTTP(S)

HTTP(S)

Config

Messages

HTTP(S)

Session Cache

Load Balancer

HTTP(S)
SSLVPN – Key Features

SSL VPN

Provide Secure access to Non-HTTP Applications
Enterprise mode (full access) or KIOSK mode (application access)
Client Integrity Check and Policy Based Access
Desktop Clean-up / Secure Folder
Architecture – SSLVPN (Server)
Architecture – SSLVPN Client (KIOSK)
Architecture – SSLVPN Client (Enterprise)

SSL VPN Client

Open VPN Client

TUN Driver

Application

User

SSL over TCP/UDP

TCP/UDP

NAM

Audit Agent

JCC

SP Agent

Conn Mgr

STunnel

Socks Server

Open VPN Server

SSL VPN

Mission Critical and Enterprise Data Systems
Recent/Current Initiatives...

Access Management On Demand
Federation Hub
Simplification
Creating products out of individual components
Simplification

Diagram showing network components such as Firewalls, DMZ, Access Gateway, Web Servers, Java Application Servers, Identity Stores, E-Mail Server, Terminal Server, SSL VPN, Private Network, L4 Switch, Access Manager Appliance(s), LDAP Server, Administration Console, and Web Servers connected in a network diagram.
How it works?
Web SSO

1. SP Agent Redirects to IdP for authentication
2. Post Credentials
3. Validate Credentials
4. IdP Redirects to SP Agent with Auth Token
5. Verify Token

If authenticated goto (4)
If not, seek credentials

Create User Session, form a token to send to SP Agent
Respond with Assertion, including user attributes/roles

Provide Access
Federated SSO

1. Request for Authentication
2. Send AuthRequest to Federated IdP
5. IdP Receives the authentication
6. Verify Token
7. Create user session and store persistent federation mapping
8. Respond with Auth Token

If authenticated goto (8)
If not, redirect to “Trusted” Federated Identity Provider
If not authenticated seek credentials
Map to Local user or Auto-provision the user.
Provide AuthResponse with authentication details
Respond with Auth Token
Protect HTTP Resources

1. Access v1.innerweb.novell.com
   - If authenticated goto (7)
   - If not, redirect to SP Agent

2. SP Agent Redirects to IdP for authentication
   - If authenticated goto (5)
   - If not, seek credentials

3. Post Credentials

4. Validate Credentials
   - Create User Session, form a token to send to SP Agent

5. IdP Redirects to SP Agent with Auth Token

6. Verify Token
   - Respond with Assertion, including user attributes/roles

7. Authorization Policy

8. Redirect to Access Resource

9. Form fill, Identity Injection, Load Balance

10. URL Rewriting, Cache
Access to Non-HTTP Resources

1. Login to SSL VPN (using IdP or AG)

2. Accept and Install Client
   - Install
   - Client Integrity Check
   - Establish VPN Tunnel
   - Client Policy Update

3. Access Enterprise Server
   - Virtual/HookingAdapter, takes request, routes through tunnel.

4. Authorize Access, Forward

5. Logout
   - Desktop Clean up

If authorized user, push the SSL VPN Client
www.novell.com/accessmanager