Service Provisioning between fixed and deployed security domains

November 2008
Table of contents

Introduction .............................................................................................................1
Oracle Service Provisioning ..................................................................................2
Proposed Solution ................................................................................................3
Further information .................................................................................................4
Introduction

UK Ministry of Defence (MoD) has multiple organisations working across many environments with users moving between organisations frequently. In order to ensure that the correct users have access to the right information from wherever they are posted, an Identity and Access Management (IdM) system is required.

IdM refers to the management of the entire lifecycle of one or more entities from creation to destruction, and managing of privileges.

One part of IdM is the provisioning of users and systems which has to be performed before services can be used and data accessed. Provisioning is the automation of the necessary processes to manage user accounts and access to systems or data. Provisioning can be done using internationally agreed standards including Services Provision Markup Language (SPML) as defined by OASIS.

Where users or systems transition between multiple organisations potentially between a fixed and a deployed infrastructure, there is a need for provisioning across the domains. As for all automatic data transfer between potentially different security domains, it is critical to ensure that only valid content is transferred and to protect the internal domain from a possible attack. Where the communication between the domains is slow or unreliable, there is a further need to make certain that the data is transferred in an efficient and reliable way.
Oracle Service Provisioning

An approach to IdM for the UK MoD DII program is described by Oracle in the paper *Oracle Identity Management Solutions for highly mobile users and organisations*. Among other things, this paper describes the use of SPML to provision users in fixed and deployed environments.

Provisioning can begin prior to deployment whilst there is an adequate link between the two (or more) domains. During this time, SPML can be used to provision the current known identities into the domain to be deployed. Oracle Identity Manager (OIM) and Oracle Web Services Manager (OWSM) combine to generate the necessary SPML message to transfer between the domains using the Oracle Enterprise Service Bus (ESB).

The transferred SPML message is then used to provision the identities in the domain to be deployed as shown in the diagram below.

Once the domain has been fully deployed, changes or new additions to the identities in the fixed domain must be propagated to the deployed domain in a strictly controlled manner. This has additional challenges when the communications links between the fixed and the deployed network are slow or unreliable and there is no permanent ESB for communications.
Proposed Solution

**Nexor Sentinel** is high assurance mail guard that is built on and enforces security targets of secure and evaluated operating systems and hardware. Currently, Nexor Sentinel runs on the Common Criteria EAL5+ evaluated STOP 6.4 / XTS-400 appliance.

Nexor Sentinel has been designed to provide a high level of assurance in cross domain environments for a wide range of sensitivity levels. Due to the diversity of the security characteristics that can be encountered between cross domain environments, Nexor Sentinel provides a simple modular approach for integration of additional applications whilst maintaining network separation. This modular approach allows Nexor Sentinel to support multiple message filters which enforce security policy.

In order to control the flow of data transferred between the fixed and deployed domains, Nexor Sentinel is able to validate the message content and can be configured to check that the content is well formed, conformant to the standards (SPML, SOAP (Simple Object Access Protocol), SAML (Security Assertion Markup Language) and contains no malicious or disallowed content. Any content failing the security policy checks will be rejected and not be passed between the two domains.

Since Nexor Sentinel supports Simple Mail Transfer Protocol (SMTP), SPML messages from the Oracle Web Services Manager carried over the ESB can use a standard SMTP connector for the ESB to communicate with the mail guard.

**Nexor Vanguard** is a tactical messaging gateway designed to support reliable IP based communications in low or unreliable bandwidth environments. It has been specifically designed to meet military requirements to enable mobile and tactical messaging. Nexor Vanguard supports SMTP messaging. It compresses the data and transfers it over User Datagram Protocol (UDP) according to the NATO standard STANAG 4406 Annex E. This provides a reliable packet oriented data transfer not offered by TCP/IP in these environments. Nexor Vanguard also supports EMCON conditions where a site cannot provide any acknowledgements due to radio silence.

Nexor Vanguard, used in conjunction with Nexor Sentinel can provide a solution to the secure provisioning of identities in the deployed space.
Further information


- Oracle Identity Management Solutions for highly mobile users and organisations, Oracle, June 2008

- Services Provisioning Markup Language (SPML) v2.0 (http://www.oasis-open.org/specs/#spmlv2.0)