"Dimitrie Cantemir" Christian University
Knowledge Horizons - Economics
Volume 11, No. 1, pp. 8 – 14
P-ISSN: 2069-0932, E-ISSN: 2066-1061
© 2019 Pro Universitaria
www.orizonturi.ucdc.ro

CHARACTERISTICS OF OPEN GRID SERVICES ARCHITECTURE

Marian Pompiliu CRISTESCU

"Lucian Blaga" University of Sibiu, Romania, Email: marian.cristescu@ulbsibiu.ro

Abstract *This paper presents the OGSA - Open Grid Services Architecture, describes the basic SOA standard of distributed Grid architectures, highlighting the architecture of the OGSA standard. There are issues related to the mobility and security of the OGSA framework, as well as the evolution of technologies involved in applying the OGSA standard to P2P environments. Grid services are described as an extension of Web service technology. In addition, the transition from the OGSI standard to the WSRF standard, is the successive implementations of the OGSA framework, is described. This also addresses the OGSA environment security issues for distributed architectures, discussing recent initiatives to create a specific and tailored OGSA environment for Web applications and security requirements specific to this transition.*

Key words:
application, architecture, security, standard, Web service
JEL Codes:
O31
O32
O33

1. INTRODUCTION

A Grid service is "a web service that provides a set of well-defined interfaces that meet certain specific conventions," that is, "a service represented by an instance of a potentially transient state, supporting secure invocations when necessary, lifetime management, notifications, policy administration, credentials, and virtualization "(A. Ripoșan et al., 2006).

The difference between OGSA and Web services is that Grid services can be managed (created, monitored, destroyed, etc.) within OGSA, and the application can obtain references to the Grid service instances that can be used for service monitoring and direct access of local data.

The reasons for building Grid services based on Web services were as follows (A. Ripoșan et al., 2005):

- Web services support discovery and dynamic composition in heterogeneous environments; WSDL is used to describe a Web service in such a way that it is independent of any specific implementation of that service.
- Web service technology is widely adopted, the scope is very broad, so there are currently a number of already existing software components and the global implementation can be achieved as needed to build a truly global Grid infrastructure.

- Web services are built on standard technologies, an important requirement for ensuring their widespread acceptance.

Grid services are focused on transient service instances, since in Grid computing, it is often necessary to create services dynamically, then and as required. Migration, for example, involves relocating job execution to a network from one machine to another while the current status of a job is saved by the "checkpointing" procedure - which typically means saving the state to a file.

OGSA defines standard mechanisms for creating, naming, discovering Grid transient instances, ensuring location transparency, and multiple protocol junctions for service instances; also supports integration with the native platform facilities on which they are built.

Virtualization of Grid services is essential for running services at a superior level on heterogeneous device collections. In a Grid environment, virtual Grid services help ensure a virtual top level across multiple Grid variants, making it possible to map / translate common semantic service functionality across multiple platforms (A. Ripoșan et al., 2005).

2. GRID SERVICES AND RESOURCES

According to OGSI specification, Grid services expanded Web services to provide additional functionality.

The main difference between OGSI - Open Grid Services Infrastructure and WSRF - Web Services Resource Framework, from this point of view, is that OGSI uses the same construction to represent a Web service and state resource, while WSRF uses another approach that separates the resource message processor.

WSRF uses the so-called predefined shape of the resource that defines the relationship between the Web services interface and resources. Any service adhering to this "default resource model" becomes a WS-Resource. The properties of a WS-Resource can be accessed through the Web service interfaces (A. Ripoșan et al., 2005).

A common feature of the two is that both OGSI and WSRF provide Web services characterized by their status for representing the components of the Grid. However, the way and the syntax in which OGSA services are defined have been changed, this not affecting the semantic behaviour of the resulting services. The functionality of an OGSI Grid service and the WSRF WS-Resource functionality are relatively similar, but the WSRF approach is more flexible and allows multi-to-many multiple-relationship relationships between Web services and any associated resource through the state.

2.1 WSRF SPECIFICATIONS

The WSRF is divided into a set of five specifications and together with the OGSI notification specification forms a set of specifications for six distinct areas (E. Deelman et al., 2008):

- WS-ResourceProperties: Describes WS-Resource and how state-related resources are associated through Web services. This specification describes how the properties

of services in the resource are accessed, how such information is altered or deleted;

- WS-ResourceLifetime: allows a user to specify a lifetime for a WS-Resource;
- WS-RenewableReferences: describes how the WS-Addressing reference, or destination address, the terminal reference, is annotated to provide the information needed to access a new reference when the current reference becomes invalid;
- WS-ServiceGroup: replaces the OGSI grouping mechanism;
- WS-BaseFault: Replaces OGSI representation for service dysfunction or exceptions;
- WS-Notification: describes asynchronous notification patterns for publish / subscription events that can be used to "remotely" listen to status changes or update service data. The WS-Notification specification has been extended to include a number of features implemented in other event notification systems.

3. ABOUT MOBILITY AND SECURITY IN THE OGSA STANDARD

There is currently a general interest in integrating mobile communication into the OGSA architecture. Some authors who have studied the limitations of Grid services in connection with mobility issues have presented some interesting aspects; these authors have proposed extending Grid services to remove these limitations (I. Foster et al., 2002).

Under the current circumstances of Grid technology development, and in line with the OGSA standard specifications, it is still difficult to decide clearly, what are the boundaries between Grid Static architectures and Grid Mobil architectures. Identifying these borders is useful to define how to differentiate between the two types of systems. Until now, the distinction has been based on whether the Grid interface is static or mobile. The mobile interface is the one that allows full virtualization of resources, and thus provides resource mobility.

According to the OGSA description, a Grid Service is static and does not have mobility, being fixed to the machine that hosts the Grid that provides that Grid service. There are many limitations that arise from the static nature of Grid services, such as the need for continuous connectivity, bandwidth, low flexibility and intelligence, and excessive service demand.

Consequently, the hypothesis that mobile Grid services can solve the problems raised by static Grid services has been issued; mobility can bring great theoretical and practical value to improve the flexibility of Grid services and increase the level of practicality.

3.1. MOBILITY OF SERVICES AND RESOURCES

The potential of resource mobility has raised the issue of resource discovery (WSRF does not specify how resources are discovered or created). If a resource is released from the endpoint / destination of the Web service and becomes essentially autonomous, resources can be

discovered and rediscovered in a decentralized manner and, moreover, when it comes to mobile resources, it is possible to discover and rediscover resources which were "lost". Therefore, a decentralized mechanism of resource discovery is needed (A. Ripoșan et al., 2006).

If the resource moves and is still exposed by another Web service, the "resolver" entity will refer the consumer to another network location. It may be necessary for the "resolver" entity to be discovered, and the "resolver" entity still needs to discover the service that now has access to the resource to get the real address (Figure 1 - b). The "resolver" entity can be notified about the location of the service, or discover the new service itself.

The address-to-execution mechanism allows services, not just resources, to migrate to different network locations, between different invitations.

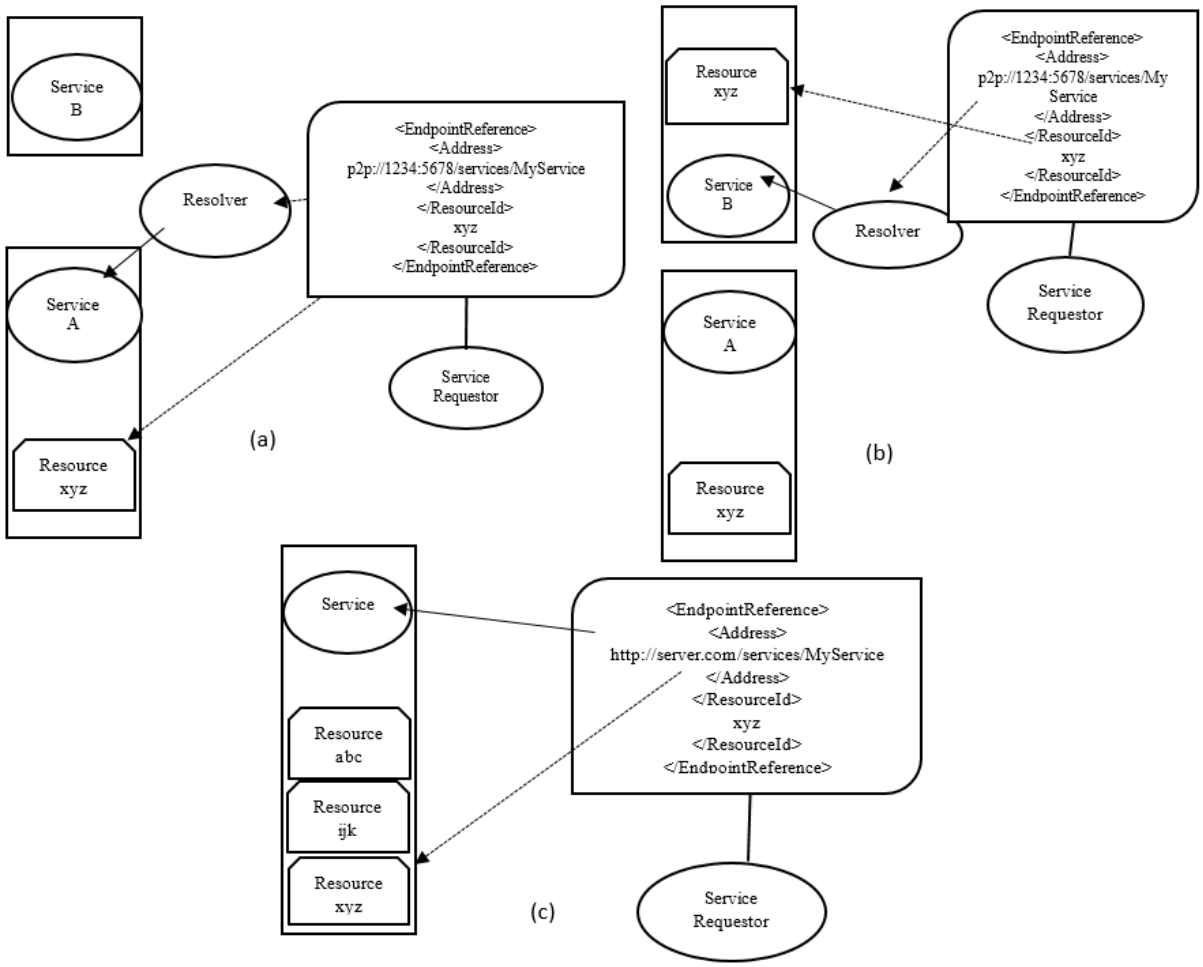
A logical destination / termination point may refer to multiple terminal / destination points, and the resolving entity may choose a particular terminal point, depending on various factors (such as network charging and response time). In addition to decoupling the service resource, a logical EPR opens the WSRF specification to a new resource class.

An example comes from the WS-ServiceGroup specification, which defines a ServiceGroup as a WS-Resource. A ServiceGroup (as a representative of a community) contains the status information about members of the group in the form of MemberEPR (which are also WS-Resources). By using logical EPRs, the responsibility of the delegated service as the Group Coordinator to maintain group membership of group members can be transferred to another service within the group. In the opposite situation, if the ServiceGroup were linked to a single service, then the whole group would cease to be operational if the private service acting as the "ServiceGroup" coordinator leaves the group, either at will or due to unforeseen circumstances. Transferring the responsibility to retain membership of "ServiceGroup" to another service within the group also requires the migration of those resources to a new location.

Another benefit of a service's ability to change its destination point is that the WSRF for services and nodes that do not have a fixed network address are open in this way (I. Wang, 2005). This category may include nodes that use DHCP to gain a network address and / or physically move over the network.

In addition, a logical terminal / destination point opens for nodes beyond NAT systems to act as service providers because the difference between the perceived terminal / destination of the service beyond NAT and the received terminal / destination as seen in the network, can be resolved at the time of execution.

Figure 1. Localization of services and resources: (a through logical addresses and the "solving" mechanism (b) Through logical addresses and the "solving" mechanism in mobility conditions, (c) without logical addresses and without the "solving" mechanism



3.2. WS-SECURITY SPECIFICATION SET

The WS-Trust (P2PS,2017) model can be used to define a framework in which Grid services can interoperate securely within a group by defining trust relationships between VO members, which ensures secure communication and at the same time makes it easy level of VO.

In the WS-Trust (P2PS,2017), each Grid Service that interfaces into a group must provide a security token to each request, which may include the name, identity, key, group, privileges, capabilities, attributes, etc. Next, a digital signature with an associated secret key can be used to demonstrate the authorized use of the security token.

WS-Security describes SOAP messaging developments to ensure the quality of data protection. WS-Security also provides a generic mechanism for associating security tokens with SOAP messages. The WS-Security specification describes how to encrypt a binary security token,

such as X.509 certificates, Kerberos vouchers, SAML assertions, etc. (UDDI Spec TC ,2018)

In addition, the WS-Trust (The WSPeer ProjectSpec TC ,2018) provides a mechanism by which the level of trust that needs to be given to assertions presented by other entities is defined and expressed at policy level: WS-Policy, WS-PolicyAttachment, and WS-SecurityPolicy (The WSPeer ProjectSpec TC ,2018).

Web Services Security Specification Set includes the following sections [39]: SOAP Message Security 1.0, Web Services Security UsernameToken Profile 1.0, Web Services Security X.509 Certificate Token Profile and relevant XML schemes.

The WSS Technical Committee for use with the SOAP Message Security 1.0 specification, including Web Services Security, provides additional token profiles: SAML Token Profile.

- SOAP Message Security 1.0 Base Specification describes SOAP protocol developments to ensure the integrity and privacy of the message. The specified mechanism can be used to be compatible with a variety of security models and encryption technologies. The specification also provides a generic mechanism for associating the security token with the content of the message. As the specification is designed to be expandable and able to support multiple tokens, no specific security tokens are required. For example, a customer can provide a token format for identity demonstration and another format to demonstrate the ownership of a certain commercial certification. Additionally, the specification describes the coding of binary security tokens, a framework for XML-based tokens, and how to include opaque encrypted keys. The specification also includes extension mechanisms that can be used to further describe the characteristics of the tokens that are included;
- The Username Token Profile document describes how to use a UsernameToken with the WSS basic specification, namely how a web service consumer can provide a UsernameToken as a means of identifying by user name, and optionally by using a password (shared secret or equivalent password); describes how that identity is authenticated with the web service provider;
- X.509 Certificate Token Profile describes how to use X.509 Certificates with the SOAP Message Security 1.0 specification. An X.509 certificate specifies a link between a public key and a set of attributes that includes at least the subject name, the name of the emitter, the serial number, and the range of validity. This link can be later revoked by mechanisms that include Certificate Revocation List (CRL), OCSP Tokens, or mechanisms outside the X.509 framework, such as XKMS. An X.509 certificate can be used to validate a public key that can be used to authenticate a rich

WS-Security message or to identify the public key through which a WS-Security-enriched message has been encrypted.

4. CONCLUSIONS

The core of WSRF specifications is the relationship between services and resources. WSRF is an attempt to reconcile the conflicting interests between service orientation and resource orientation.

Under the new approach, a service within the WSRF is not explicitly linked to a resource instance but is instead declared for a certain type of resource; through which a resource can maintain its "state" while the service that exposes resources remains "without state".

A service - during transmission of the message - can manipulate the state, a security context and a "workflow" context; consequently, the state (as implemented in the WSRF) can only be considered as another context that is handled by the service. The concept of context is important in SOA architectures that tend towards "gentle couplings" between entities, the context allowing all information related to the transmission of a message to be included in that message.

REFERENCES

- Ripoșan, A. Harrison, I. Taylor, I. Kelley, and E. Mieilica, (June 6-9.,2006) "Mobile peer-to-grid architecture for paramedical emergency operations", in Proceedings of HealthGrid 2006 - Challenges and Opportunities of HealthGrids, IOS Press, Valencia, Spain.
- Ripoșan, I. Taylor, and Y. Legre, (August 28-30, 2006) , "Identifying mobile grid scenarios for medical imaging applications", in MIE 2006, Poster Session - Decision Support, Knowledge Representation and Management, Maastricht, The Hague.
- Ripoșan and V. Patriciu, (November 2005)" Grimi, grid-enabled research infrastructure for medical imaging", in Modern Technologies in the XXI Century, Bucharest, Romania.
- Ripoșan and V. Patriciu, (November 2005), "Mobile grid infrastructure, a proposal for a MTA integrated Project", in Modern Technologies in the XXI Century, Bucharest, Romania.
- E. Deelman, D. Gannon, M. Shields, and I. J. Taylor, (July 2008) „Workflows for e-Science: An overview of workflow system features and capabilities", Journal of Future Generation Computer System,
- Foster, C. Kesselman, J. Nick, and S. Tuecke, (June 2002) „The physiology of the grid: An open grid services architecture for distributed systems integration", Open Grid Service Infrastructure WG, Global Grid Forum.
- Wang,"P2PS (Peer-to-Peer Simplified)",(February 2005) in Proceedings of 13th Annual Mardi Gras Conference-Frontiers of Grid Applications and Technologies, pp.54–59, Louisiana State University.
- P2PS - Peer-to-Peer Simplified. (Dec.10 2017) Available on-line at : http://www.trianacode.org/p2ps/.
- (Feb. 21, 2018).The WSPeer Project, Available on-line at : http://www.wspeer.org/.
- UDDI Spec TC, UDDI Version 3.0.2, (September 2004), Available on-line at : http://uddi.org/pubs/uddiv3.htm, [Ian. 18, 2018].