Authors:
Glenn Wasson, UVA
Marty Humphrey, UVA

http://forge.gridforum.org/projects/ogsa-hpcp-wg

11/30/2007

HPC File Staging Profile, Version 0.1

Status of this Memo

This memo provides information to the Grid community regarding the specification of the HPC File Staging Profile. Distribution is unlimited.

Copyright Notice

Copyright © Open Grid Forum (2007). All Rights Reserved.

Abstract

This document profiles the File staging capabilities of the Job Submission Description Language (JSDL) for use by HPC Basic Profile-compliance services. It includes clarifications, refinements, interpretations and amplifications of JSDL which promote interoperability.

Contents

Abstract 1

1 Introduction 3

2 Notational Conventions 3

3 JSDL Data Staging 3

3.1 JSDL 1.0 Data Staging Elements 3
3.1.1 FileName 3
3.1.2 FileSystemName 4
3.1.3 CreationFlag 4
3.1.4 DeleteOnTerminate 4
3.1.5 Source 4
3.1.6 Target 4

3.2 Credentials 4

3.3 Supported Protocols and Security Tokens 4

3.4 File Staging Failure Semantics 5

4 HPC File Staging Profile Service State Model 5

4.1 File Transfer Errors 5

4.2 File Staging Errors 6

5 Author Information 7

6 Contributors 7

7 Acknowledgements 7

8 Full Copyright Notice 7

9 Intellectual Property Statement 7

10 Normative References 8

1 Introduction

The HPC File Staging Profile is a document that is used to describe an extension to the HPC Basic Profile [ref]. This profile addresses how file staging can be performed by HPC Profile-compliant services using the JSDL <DataStaging> directives.

The Profile consists of references to existing specifications, along with any clarifications of the contents of those specifications, restrictions on the use of those specifications, and references to any normative extensions to those specifications. While it is envisioned that many systems will have capabilities above and beyond those described in this profile, this profile describes a basic set of capabilities that can be used as the basis of interoperability testing between systems claiming compliance.

The document is structured as a set of sections, each of which is used to reference a particular aspect of an HPC File Staging Profile compliant system.

2 Notational Conventions

The key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in RFC-2119 [RFC 2119].

The document refers to an “HPC File Staging Profile compliant system” as a “Compliant system”.

This specification uses namespace prefixes throughout; they are listed in Table 2-1. Note that the choice of any namespace prefix is arbitrary and not semantically significant.

Table 2-1: Prefixes and namespaces used in this specification.

Prefix	Namespace
xsd	http://www.w3.org/2001/XMLSchema
jsdl	http://schemas.ggf.org/jsdl/2005/11/jsdl
bes-factory	http://schemas.ggf.org/bes/2006/08/bes-factory
hpcp-bp	http://schemas.ogf.org/hpcp/2007/01/bp
hpcp-fs	http://schemas.ogf.org/hpcp/2007/01/fs

3 JSDL Data Staging

This profile adopts the DataStaging elements from the Job Submission Description Language v1.0 [JSDL10]. Modifications and clarifications to those elements appear in section 3.1. In addition, the profile extends these elements by defining an additional element that may be used by clients for scheduling data transfers.

3.1 JSDL 1.0 Data Staging Elements

A system compliant with this profile must support the JSDL data staging elements with the following modifications.

3.1.1 FileName

As in [JSDL10].

3.1.2 FileSystemName

This profile does not mandate support for this element. Compliant systems which receive a file staging request containing a <FileSystemName> element may return a fault. Such systems may also return a fault if a FileSystem is defined in the <Resources> element of a received JSDL document.

3.1.3 CreationFlag

As in [JSDL10], but with the clarification that it is not considered an error if the CreationFlag is set to dontOverwrite and a file with the same name exists at the target location.

3.1.4 DeleteOnTerminate

As in [JSDL10]. However, this profile defines that failure to delete the file will move the job to the Failed state (see section 4).

3.1.5 Source

As in [JSDL10].

3.1.6 Target

As in [JSDL10].

3.2 Credentials

Files staging operations may require additional credentials in order to interact with remote systems. This profile defines an additional element, called <Credential> which can be placed in the <DataStaging> element. The value of this element is <xsd:any> and an example of this is shown below.

```
<DataStaging>
   <FileName>output.txt</FileName>
   <CreationFlag>overwrite</CreationFlag>
   <Target>
       <URI>ftp://server.inthe.sky:1234</URI>
   </Target>
   <Credential xmlns="http://schemas.ogf.org/hpcp/2007/11/ac">
       <UsernameToken xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
           <Username>demo</Username>
           <Password>pass</Password>
       </UsernameToken>
   </Credential>
</DataStaging>
```

3.3 Supported Protocols and Security Tokens

While JSDL defines schema types for data staging elements, it does not further specify permissible values. This profile, in contrast, requires compliant systems to support a minimum set of values for those elements. Specifically, this profile requires that compliant services support at least one of the following file transfer protocols: ftp, http and scp. These protocols will likely be referenced by clients using the scheme portion of the <URI> sub-elements (e.g. ftp://) within both the <Source> and <Target> elements.

In addition, while the schema type of the <Credential> element is <xsd:any>, compliant services must support the inclusion of at least one of WS-Security UsernameTokens [WSSUTP] or WS-Security X.509 CertificateTokens [WSSX509] within this element.

3.4 File Staging Failure Semantics

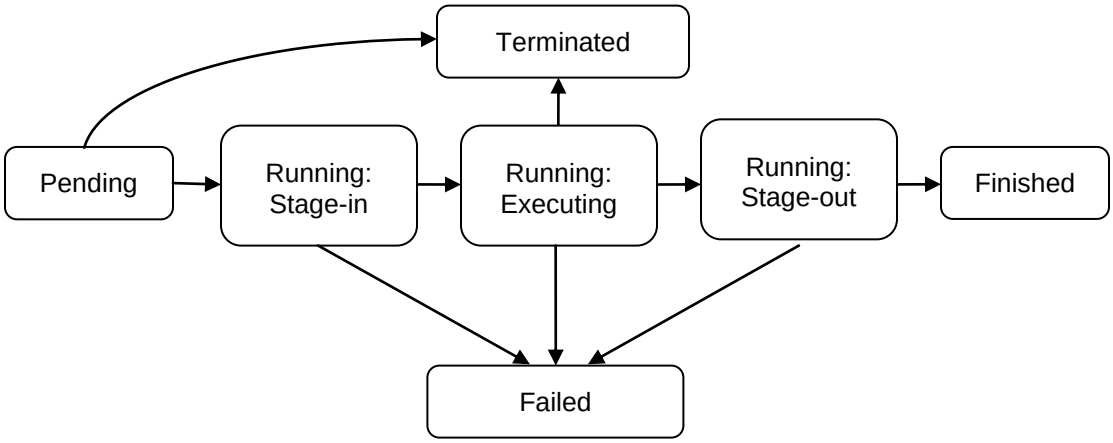
A JSDL document may specify that multiple files must be staged-in and/or staged-out. This leaves open two questions: 1) whether the job is considered to be in error if some (but not all) of those staging requests fail and 2) how should any staging operations that are in-process or not yet started be handled once a failure occurs? In other words, should a job trasition to the “failed” state as soon as any staging directive fails and should staging operations continue after a failure occurs? The later in particular may have different answered for the stage-in and stage-out cases. For stage-in, it may be reasonable to stop staging once a file transfer fails (under the assumption that the job will not be able to run without all of its input data available), while for stage-out it may be reasonable to attempt to stage-out every requested file even if some fail.

Since undoubtly services complying with this profile will be based on infrastructures with diverse failure models/semantics, this profile places no mandate on the semantics of failure in multiple data staging operations. A service MAY transition to the failed state when a data staging failure occurs. In addition, a service MAY abort current and/or uninitiated transfers when a staging failure occurs. Finally, a service MAY support extensions to this profile by which clients can specify a particular set of desirable semantics.

4 HPC File Staging Profile Service State Model

While the definition of errors is outside the scope of JSDL, it is within scope for a service enacting file transfer operations. Since this profile extends the HPC Base Profile, which uses the BES state model, we extend that model to include new states for stage-in/stage-out file transfer.

The new state diagram is shown below.



4.1 File Transfer Errors

While the above state model provides distinct state transitions for errors related to staging-in, staging-out and executing, these transitions may occur for many different reasons. In order to more precisely describe the source of failure to clients, this profile extends the ActivityStatusType defined in BES [BES10] to include fault information (using the built-in extensibility of that element). An example message is shown below:

```
<bes-factory:GetActivityStatusesResponse>
   <bes-factory:ActivityIdentifier>
      <wsa:Address>http://tempuri.org/some-service</wsa:Address>
      <wsa:ReferenceParameters>
         <n00:id>D4A88953-FFFF-49F6-5145-AE21FF0438AE</n00:id>
      </wsa:ReferenceParameters>
   </bes-factory:ActivityIdentifier>
   <bes-factory:ActivityStatus>
      <bes-factory:State>Failed</bes-factory:State>
      <soap:Fault>
         <soap:faultcode> some code </soap:FaultCode>
         <soap:detail> a fault description, e.g. a fault schema from section 4.2 </>
      </soap:Fault>
   </bes-factory:ActivityStatus>
</bes-factory:GetActivityStatusesResponse>
```

A SOAP 1.1 fault has been added to the <bes-factory:ActivityStatus> element. This fault could describe the source of the stage-in failure, e.g. insufficient disk space or unknown source file. Note that this fault is different from the Fault element which may be present as a sub-element of the <bes-factory:GetActivityStatusesResponse> element. While the later indicates that a fault occurred in querying the status of an activity, the former provides details useful to determining why the activity is in its current failure state.

4.2 File Staging Errors

We define the following standard error types that can be placed in the <detail> element of the SOAP faults introduced in section 4.1. It should be noted that determining the cause of a file transfer failure can be difficult particularly when the error occurs on a remote system. As such, these error message should be used when an appropriate cause for the error can be determined, but it is not mandatory to throw one of these errors.

UnknownFileFault – this fault should be thrown when the file indicated by the <Source> element or the remote server/directory indicated by the <Target> element cannot be found.

```
<hpcp-fs:UnknownFileFault>
   <hpcp-fs:File> xsd:anyURI </hpcp-fs:File>
</hpcp-fs:UnknownFileFault>
```

UnsupportedProtocolFault – this fault should be thrown when the file indicated by the <Source> or <Target> element specifies a transfer protocol that is not supported by the service. The <File> sub-element indicates the file who's URI contains the unsupported protocol.

```
<hpcp-fs:UnsupportedProtocolFault>
   <hpcp-fs:File> xsd:anyURI </hpcp-fs:File>
</hpcp-fs:UnsupportedProtocolFault>
```

NotAuthorizedFault – this fault, defined in BES 1.0 [BES10], should be thrown when the stage-in or stage-out requests cannot be completed due to insufficient permissions of the entity performing the staging operation.

InsufficientStorageSpaceFault - this fault should be thrown when a stage-in operation cannot complete due to insufficient storage space in the location on the local system where the remote file is being written. It should also be thrown when there is insufficient space available on the target machine for a stage-out request. The <File> subelement indicates the file being staged when the error occurred.

```
<hpcp-fs:InsufficientStorageSpaceFault>
   <hpcp-fs:File> xsd:anyURI </hpcp-fs:File>
</hpcp-fs:InsufficientStorageSpaceFault>
```

DeleteOnTerminationFault – this fault should be thrown if a staging request has the DeleteOn-Termination flag set to true and the service is unable to delete the specified file. The <File> sub-element indicates the file while was not deleted.

```
<hpcp-fs:DeleteOnTerminationFault>
   <hpcp-fs:File> xsd:anyURI </hpcp-fs:File>
</hpcp-fs:DeleteOnTerminationFault>
```

5 Author Information

Glenn Wasson
University of Virginia

Marty Humphrey
University of Virginia

6 Contributors

We gratefully acknowledge the contributions made to this specification by [insert names].

7 Acknowledgements

We are grateful to numerous colleagues for discussions on the topics covered in this document, in particular (in alphabetical order, with apologies to anybody we've missed) [insert names].

We would like to thank the people who took the time to read and comment on earlier drafts. Their comments were valuable in helping us improve the readability and accuracy of this document.

8 Full Copyright Notice

Copyright © Global Grid Forum (2003-2005). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the GGF or other organizations, except as needed for the purpose of developing Grid Recommendations in which case the procedures for copyrights defined in the GGF Document process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the GGF or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE GLOBAL GRID FORUM DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

9 Intellectual Property Statement

The GGF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made availa-

ble, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the GGF Secretariat.

The GGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this recommendation. Please address the information to the GGF Executive Director (see contact information at GGF website).

10 Normative References

[RFC 2119] Bradner, S. *Key words for use in RFCs to Indicate Requirement Levels*. Internet Engineering Task Force, RFC 2119, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt

[JSDL10] Available at http://www.ggf.org/documents/GFD.56.pdf.

[BES10] Available at http://www.ogf.org/documents/GFD.108.pdf.

[HPCP10] Available at

[WSSUTP] Nadalin, A., Griffin, P., Kaler, C., Hallam-Baker, P., and Monzillo, R. eds. *Web Services Security UsernameToken Profile 1.0*. March 2004. Available at http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0.pdf.

[WSSX509] Hallam-Baker, P., Kaler, C., Monzillo, R., Nadalin, A. eds. *Web Services Security X.509 Certificate Token Profile 1.0*. March 2004. Available at http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf.