# TABLE OF CONTENTS

- Legal Notice .............................................................................................................................................................................. 3
- Executive Summary ....................................................................................................................................................................... 4
- Purpose .................................................................................................................................................................................................... 5
- Taxonomy .................................................................................................................................................................................................. 5
- Assumptions .................................................................................................................................................................................................. 6
- Long Distance Workload Migration Usage Scenarios ...................................................................................................................... 7
  - General Migration Classes .......................................................................................................................................................... 7
  - Representative Migration Use Models ........................................................................................................................................ 8
    - What is a Workload? ......................................................................................................................................................................... 8
    - General Migration Workflow ....................................................................................................................................................... 9
- Usage Scenario 1 – Data Affinity .................................................................................................................................................... 9
- Usage Scenario 2 – Follow-the-Sun ................................................................................................................................................ 10
- Usage Scenario 3 – Disaster Recovery ........................................................................................................................................... 12
- Usage Scenario 4 – Follow-the-Moon .............................................................................................................................................. 13
  - Usage Scenario Variation – Lazy Follow the Sun .......................................................................................................................... 14
- Usage Scenario 5 – Cloud Bursting ................................................................................................................................................. 14
  - Usage Scenario Variation – Franchise Deployment .......................................................................................................................... 15
  - Usage Scenario Variation – Elastic Load Balancing ........................................................................................................................ 15
- Usage Scenario 6 – Disaster Avoidance ........................................................................................................................................ 16
  - Usage Scenario Variation – Data Center Closure .......................................................................................................................... 16
- Service Tiers ............................................................................................................................................................................................ 17
- RFP Requirements – Solution Providers ........................................................................................................................................... 19
- RFP Requirements – Service Providers ........................................................................................................................................... 19
- Summary of Industry Actions Required ........................................................................................................................................... 20
LEGAL NOTICE

© 2012 Open Data Center Alliance, Inc. ALL RIGHTS RESERVED.

This “Open Data Center AllianceSM Usage Model: Long Distance Workload Migration” is proprietary to the Open Data Center Alliance, Inc.

NOTICE TO USERS WHO ARE NOT OPEN DATA CENTER ALLIANCE PARTICIPANTS: Non-Open Data Center Alliance Participants only have the right to review, and make reference or cite, this document. Any such references or citations to this document must give the Open Data Center Alliance, Inc. full attribution and must acknowledge the Open Data Center Alliance, Inc.’s copyright in this document. Such users are not permitted to revise, alter, modify, make any derivatives of, or otherwise amend this document in any way.

NOTICE TO USERS WHO ARE OPEN DATA CENTER ALLIANCE PARTICIPANTS: Use of this document by Open Data Center Alliance Participants is subject to the Open Data Center Alliance’s bylaws and its other policies and procedures.

OPEN CENTER DATA ALLIANCESM, ODCA SM, and the OPEN DATA CENTER ALLIANCE logoSM are service marks owned by Open Data Center Alliance, Inc. and all rights are reserved therein. Unauthorized use is strictly prohibited.

This document and its contents are provided “AS IS” and are to be used subject to all of the limitation set forth herein.

Users of this document should not reference any initial or recommended methodology, metric, requirements, or other criteria that may be contained in this document or in any other document distributed by the Alliance (“Initial Models”) in any way that implies the user and/or its products or services are in compliance with, or have undergone any testing or certification to demonstrate compliance with, any of these Initial Models.

Any proposals or recommendations contained in this document including, without limitation, the scope and content of any proposed methodology, metric, requirements, or other criteria does not mean the Alliance will necessarily be required in the future to develop any certification or compliance or testing programs to verify any future implementation or compliance with such proposals or recommendations.

This document does not grant any user of this document any rights to use any of the Alliance’s trademarks.

All other service marks, trademarks and trade names referenced herein are those of their respective owners.

Published April, 2012
EXECUTIVE SUMMARY

Historically, workload migration over any distance has been an immensely complex, time consuming and disruptive activity. With the adoption of virtualization at the core of modern infrastructure services, the complexity of the underlying infrastructure may have increased between but the potential to eliminate time and disruption from migration activities is finally possible, albeit currently somewhat constrained by relatively short distances and low latencies.

The drivers for long distance workload migration capabilities are really no different from those that led to the current state of technology, which can be considered in terms of three foundational classes: migration, extension and sustaining. This document presents six practical usage models based on these classes, along with success and failure scenarios for each. Finally, a discussion of service provider requirements and an industry call to action is presented.

This document serves a variety of audiences. Business decision makers looking for specific solutions, and enterprise IT groups involved in planning, operations, and procurement will find this document useful. Solution providers and technology vendors will benefit from its content to better understand customer needs and tailor service and product offerings. Standards organizations will find the information helpful in defining end-user relevant and open standards.
PURPOSE

There are several motivations for long distance workload migration. Business drivers typically fall into one of several categories (see also Travostino, et al 2005):

- **Business Continuity**: Migrate or replicate workloads to establish an orderly evacuation of a data center that has experienced, or anticipates experiencing failures, security breaches, or other disruptions. This encompasses both disaster recovery and disaster avoidance. Seasonal migrations of workloads in high-risk areas would also be included here.

- **Resource Locality**: It is impossible, impractical, or too costly to bring data, or other resources, close to the compute environment. So, move the application and services closer to the needed resources. This could be driven by data volume, device requirements, power costs (*Follow-the-moon*), data residency requirements, or other legal/regulatory restrictions.

- **Follow-the-sun**: Move workloads close to users based on geographic locations, time zone considerations, etc. This is performed on a proactive and scheduled basis. *Follow-the-sun* is a special variant of resource locality where the users are the “resource” the workload needs to be close to.

- **Dynamic Scaling**: May also be referred to as data center expansion or cloud bursting. It is the need to dynamically and elastically acquire and dispose of capacity. We include both real-time, on-demand and proactively scheduled scaling. The benefit is that the clients (cloud subscribers) should no longer have to build for peak demand.

- **Data Center Migration**: Move workloads to a new facility because the cloud subscriber is temporarily or permanently changing facilities. This could be driven by a data center consolidation program or by termination of a relationship with a given cloud provider, for example.

Note: Compute and cloud marketplaces are currently out of scope for this usage model.

TAXONOMY

<table>
<thead>
<tr>
<th>Actor/Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Provider</td>
<td>An organization providing network services and charging cloud subscribers. A (public) cloud provider provides services over the Internet. A cloud subscriber could be its own cloud provider, such as for private clouds.</td>
</tr>
<tr>
<td>Cloud Standards Body</td>
<td>An entity responsible for setting and maintaining the cloud orchestration standards contemplated in this usage model.</td>
</tr>
<tr>
<td>Cloud Subscriber</td>
<td>A person or organization that has been authenticated to a cloud, and maintains a business relationship with a cloud.</td>
</tr>
<tr>
<td>Long Distance</td>
<td>For the purposes of this usage model, long distance is defined as greater than 20km of conductor between disparate data centers (cloud provider sites). Inter-site latency is assumed to be at least 10ms or worse.</td>
</tr>
<tr>
<td>Migration—At Rest</td>
<td>At-rest migration allows the transfer of a fully-stopped virtual machine (VM) instance or a machine image from one provider site to another site, or between disparate providers. It also may include migrating applications, services, and their contents from one site (or provider) to another. By definition, only one site may accept connections for the subject workload at a time. This is also referred to as <em>cold</em> migration. (See National Institute of Standards and Technology (NIST) Cloud Computing Reference Architecture ².)</td>
</tr>
</tbody>
</table>

¹ http://dl.acm.org/citation.cfm?id=1160266
Migration—Live

Live migration approximates continuous operation of a set of processes even as they are being sent to another physical location. This may also be referred to as hot migration. ([Travostino, et al 2005](#)). The user of the workload is not impacted, with no downtime in his or her service.

Traffic Trombone

Network traffic between disparate data centers caused by separated workload components during a live migration.

Workload

This document uses the following technical workload definitions:

- For Compute Infrastructure as a Service (ClaaS) clouds, a workload equals a virtual machine instance or machine image together with the needed information about the technical layout (e.g., number of cores, RAM, and so on), network configuration and the data store directly associated with the VM. The VM is the abstraction of all the workload’s constituent elements.

- For Storage as a Service (StaaS), the workload is just the data—effectively a degenerate case of ClaaS.

- For Platform as a Service (PaaS) clouds, the workload is based on the same information as for ClaaS, plus an abstraction of application processes, data, configuration, state, and the relationships associated with them. This takes the form of different application stacks.

ASSUMPTIONS

The following assumptions apply to the usage scenarios contained herein:

1. Where cloud provider and cloud subscriber are separate legal organizations, there is a properly executed service agreement similar to the Commercial Services Framework from the Open Data Center Alliance (ODCA).

2. Cloud providers implement the [ODCA Service Catalog Usage Model](#).

3. Adherence to the Distributed Management Task Force (DMTF) [Open Virtualization Format](#) (OVF) specification.

4. Compliance with [ODCA VM Interoperability Usage Model](#), including import and export of VM packages per OVF.

5. For extension and sustaining foundational class “migrations,” we assume the applications built on cloud provider services follow the practices of the [ODCA Whitepaper Developing Cloud-Capable Applications](#). Note: migration class migrations do not depend on this assumption.

6. Service Level Agreements (SLA), Operating Level Agreements (OLA), and relevant controls are specified between the cloud provider and cloud subscriber. These may include:

   - Type of migration capabilities required
   - At-rest vs. live migration
   - Availability
   - Security root of trust
   - Consistency of management

---


5 [www.dmtf.org/standards/ovf](www.dmtf.org/standards/ovf)


• Security and compliance
• Carbon measurement
• Geographic hosting requirements
• Workload owner, roles and responsibilities of relevant parties
• Roll-back criteria
• Duration of roll-back availability

7. All clocks are synchronized to UTC time.
8. Workloads can be stopped for at-rest migration.
9. Each workload can be described in a “manifest.” The manifest is simply a list and dependency mapping of all relevant workload components and requirements. (A manifest implementation format is beyond the scope of this usage model).
10. Unless specified otherwise, all migrations occur between disparate data centers of the same cloud provider.
11. Workload migrations are initiated based on the cloud subscriber’s intent, either explicitly by the subscriber or automatically, based on a subscriber-defined policy.
12. Unless specified otherwise, connectivity between source and target data centers is over the public internet.

LONG DISTANCE WORKLOAD MIGRATION USAGE SCENARIOS

GENERAL MIGRATION CLASSES

There are three generic classes from which specific workload migration usage scenarios can be built. These classes can help address specific business usage scenarios not yet encountered, and provide a way to generalize implementations. These generic workload migration classes are as follows:

• **Relocate**: Implies the workload can be at only one place at a time. It can be thought of as moving the workload.
• **Extend**: Extends the workload into new places. It can be thought of as growing the workload.
• **Sustain**: Sustains the workload. It can be thought of as preserving or keeping the workload.

Relocating a workload allows a workload to move from one location to another. Pure migration implies being operational at only one place at a time. It does include geographic diversity and potential fault detection, but does not include elements of load distribution or horizontal scalability. Relocation can address disaster recovery sustainability with planning, pre-placement, and failure detection mechanisms.

Extending a workload extends a function into additional geographic and/or network topological locations. It includes elements of geographic diversity, horizontal scalability, and a load distribution mechanism (i.e., global load balancer). Increased capacity, throughput and performance are common goals of workload extension. Extend could also be used to gradually vacate unneeded sites as well.

Sustaining a workload provides for continuity of operation during and after an event. Elements of workload sustainability include: geographic diversity, horizontal scalability (support for multiple instances), and a load distribution mechanism (i.e., global load balancer). Increased availability is the goal. Sustaining workloads is analogous to the Internet routing around damage, and can address disaster avoidance requirements.
Representative Migration Usage Scenarios

Recall the business drivers explained in the “Purpose” section of this document. Each of those business drivers can be addressed by at least one of the above migration classes. See the table below for which migration class can be used to address each business driver. Where a given migration class can be applied to a business driver, a sample usage scenario is indicated. Empty cells indicate where a migration is not applicable.

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Relocate</th>
<th>Extend</th>
<th>Sustain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity</td>
<td>Usage Scenario 3 – Disaster Recovery</td>
<td></td>
<td>Usage Scenario 6 – Disaster Avoidance</td>
</tr>
<tr>
<td>Resource Locality</td>
<td>Usage Scenario 1 – Data Affinity</td>
<td>Usage Scenario 4 – Follow-the-Moon</td>
<td></td>
</tr>
<tr>
<td>Follow-The-Sun</td>
<td>Usage Scenario 2 – Follow-the-Sun</td>
<td>Usage Scenario 4 – Lazy-Follow-the-Sun Variant</td>
<td></td>
</tr>
<tr>
<td>Dynamic Scaling</td>
<td></td>
<td>Usage Scenario 5 – Cloud Bursting</td>
<td></td>
</tr>
<tr>
<td>Data Center Migration</td>
<td></td>
<td></td>
<td>Usage Scenario 6 – Data Center (DC) Closure Variant</td>
</tr>
</tbody>
</table>

Specific examples for each of the situations in the table above are addressed in the usage scenario section. Note that there is some overlap in which more than one migration class can meet a given business driver. Depending on the specific business requirements of a given situation, there may be more than one solution.

Workload migration is a fundamental requirement in many different kinds of business situations. It would be impossible to enumerate each potential such usage scenario. The six examples included herein are representative of commonly observed business requirements. There are, of course, other variations. Cloud subscribers can articulate these in a common manner using the workflow steps described in the “General Migration Workflow” section below.

All of the use cases are applicable to private, community, public, and hybrid clouds.

What is a “Workload?”

Generically speaking, a workload is an encapsulation of one or more of the following: application processes, data, configuration information, and state. This also includes metadata that describes the relationships amongst those elements.

For Infrastructure as a Service (IaaS) services, the abstraction for a workload is the virtual machine (may or may not include the container). For PaaS services, there is no uniformly agreed abstraction yet, although they are built on top of IaaS constructs. In practice, however, PaaS workloads may often be manifested as an application stack.

For this document, unless specified otherwise, PaaS workloads assume the “Basic” and “Complex” application stack examples from the ODCA Identity Management Interoperability Guide, specifically:

- **Simple Web Application**: A simple enterprise application could be defined programmatically in the Java/JEE context as a single EAR/WAR [JEE] file. This simple application would leverage the following components: persistence [database], automation [provisioning], and security frameworks application programming interfaces (APIs). This application would consume the components from a single platform provider.
• **Complex Web Application**: A complex enterprise application would be defined in the Java/JEE context as multiple WAR/EAR files, and could consume components across both public (cloud provider) and private (cloud subscriber) clouds. These components would include all aspects of a typical enterprise application, including caching (distributed/local), persistence (SQL/noSQL), and automation (dynamic/scheduled scaling).

**GENERAL MIGRATION WORKFLOW**

The Migrate, Extend, and Sustain classes each have distinct workflow steps, while also having many in common. Variations on workflow implementation can be used to address niche cloud subscriber requirements not contemplated herein. First, some additional definitions follow:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The site or data center where the workload is originally located.</td>
</tr>
<tr>
<td>Target</td>
<td>The site or data center where the workload is to be moved or copied.</td>
</tr>
<tr>
<td>Control</td>
<td>Short-hand for which site or data center is, at that moment, the primary location for the subject workload. This could be the source, the target, or a load balancing facility.</td>
</tr>
</tbody>
</table>

A general workflow framework is illustrated below, and specific usage scenario examples follow. To be clear, by workflow here we are referring to the migration process itself. One way to think of the general workflow is as a set of migration building blocks that can be assembled for a given business usage scenario. Proper implementation of the migration workflow is dependent upon good orchestration solutions, which are preferably standardized among cloud providers.

**Note**: Maybe means that the migration step depends on specific business requirements.

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Applicable to Migration Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step # Migration Step</td>
<td>Relocate Extend Sustain</td>
</tr>
<tr>
<td>1  Prepare source workload for migration.</td>
<td>Yes</td>
</tr>
<tr>
<td>2  Marshal resources and set up environment at the target.</td>
<td>Yes</td>
</tr>
<tr>
<td>3  Provision processes at the target.</td>
<td>Yes</td>
</tr>
<tr>
<td>4  Provision data at the target.</td>
<td>Yes</td>
</tr>
<tr>
<td>5  Copy state to the target.</td>
<td>Maybe</td>
</tr>
<tr>
<td>6  Confirm successful process and data provisioning.</td>
<td>Yes</td>
</tr>
<tr>
<td>7  Assign control to the target.</td>
<td>Yes</td>
</tr>
<tr>
<td>8  Destroy or disengage the source.</td>
<td>Yes</td>
</tr>
<tr>
<td>9  Accept new connections at the target.</td>
<td>Yes</td>
</tr>
<tr>
<td>10 Balance connections between the source and the target.</td>
<td>No</td>
</tr>
</tbody>
</table>

**USAGE SCENARIO 1 — DATA AFFINITY**

• **Motivation**: Resource Locality

• **Migration Class**: Relocate

The example for Usage Scenario 1 is motivated by a requirement to perform compute operations on data that is already in place. This could be because the cost of moving the data is significantly higher than the cost of compute. This could also apply where other resources were required, such as specific devices or low-cost power (see Follow-the-Moon, Usage Scenario 4, for another example of resource-driven affinity). The requirements may be exacerbated by a need to maintain state across the compute, and/or by algorithm constraints. Below is a specific example, paraphrased from *Travostino, et al 2005*:

© 2012 Open Data Center Alliance, Inc. ALL RIGHTS RESERVED.
An iterative search for patterns embedded in digital images stored across multiple and distant data centers. Virtual machines at each of the data centers are loaded with the necessary applications and environment. A live migration will allow the applications to move close to the image sets and thus access the right data at the right time, with lowest possible latency.

Below are the high-level steps for using the Relocate class to implement data affinity using live migration. This assumes the same cloud provider at source and target.

1. Construct a manifest of all workload components and requirements at the source site. This could be done by either the cloud subscriber or cloud provider, depending upon their contract and SLA. This manifest will be used in the orchestration of the remaining steps.

2. The cloud provider will deploy all required software applications and system components to the target site.

3. The cloud provider will replicate storage/data to the target site.

4. The cloud provider will execute a live migration of the workload.

5. Once the live migration is confirmed complete and correct, the cloud provider will redirect traffic to the target site.

6. All Quality of Service (QoS), performance, security, and availability characteristics at target must be at parity with the source, unless otherwise agreed upon by the cloud subscriber.

Steps 3 through 5 should be treated as an atomic event. That is, they should be guaranteed either to occur completely or have no effect. Migration failure during any of those steps should cause a full rollback and continuation to operate with the in-place resources.

Success Scenario 1:
The workload is moved to the target without interruption to workload execution, and without disruption to state.

Failure Condition 1:
The migration was interrupted or not possible. The migration did not complete successfully, and therefore the workload is unable to enter running state at the target. Roll back to the source site and Return Error code are expected to allow for retry or failure event notice.

Failure Condition 2:
The migrated workload cannot be started, and does not work as intended. The migration completed successfully. However, the workload is unable to enter running state due to various failure conditions. Roll back to the source site and Return Error code are expected to allow for roll back and retry, or failure event notice.

Failure Condition 3:
The migrated workload does not perform as expected. The migration completed successfully and the workload entered a running state at the target site. However, workload behavior and/or user experience is incorrect due to various failure conditions. The cloud subscriber raises an incident to the cloud provider.

Failure Condition 4:
The cloud provider cannot meet the usage scenario goals without introducing unacceptable risks such as network broadcast storms or network loops.

Usage Scenario 2 – Follow-the-Sun

- **Motivation:** Follow-the-sun
- **Migration Class:** Relocate

The example in Usage Scenario 2 is motivated by a cloud subscriber’s need to move content and capability close to users through the course of a 24-hour day. In some cases, peaks and troughs in workload volumes are highly correlated to the time of day, especially in the case of...
user-facing applications. Basically, follow-the-sun models leverage cloud ubiquity to move or relocate applications to be used globally. This allows workloads to be delivered to the right place at the right time.

Note: This usage scenario assumes a hard cut-over of workloads from source to target. A more advanced version of follow-the-sun is contemplated as a variation to Usage Scenario 4 of this usage model.

Below are the high-level steps for using the Relocate migration class to implement follow-the-sun:

1. Construct a manifest of all workload components and requirements at the source site. This could be done by either the cloud subscriber or cloud provider, depending upon their contract and SLA. This manifest will be used in the orchestration of the remaining steps.
2. Cloud provider will deploy all required software applications and system components to the target site.
3. The cloud provider will replicate storage to the target site.
4. The cloud provider will execute a migration of the workload.
5. Once the workload migration is confirmed complete and correct, the cloud provider will redirect traffic to the target site.
6. All QoS, performance, security, and availability characteristics at target must be at parity with the source, unless otherwise agreed by cloud subscriber.

Note that steps 3 through 5 above should be treated as an atomic event. Migration failure during any of those steps should cause a full rollback and continuation to operate with the in-place resources.

Choice of at-rest or live migration is a business decision. However, if the migration is according to pre-determined policies and plans, then at-rest migration may be appropriate.

Success Scenario 1:
The workload is added at target successfully. Connections are successfully directed to the target.

Failure Condition 1:
The migration was interrupted or not possible. The migration did not complete successfully, and therefore the workload is unable to enter running state at the target. Roll back to the source site and Return Error code are expected to allow for retry or failure event notice.

Failure Condition 2:
The migrated workload cannot be started and does not work as intended. The migration completed successfully. However, the workload is unable to enter running state due to various failure conditions. Roll back to the source site and Return Error code are expected to allow for roll back and retry or failure event notice.

Failure Condition 3:
The migrated workload does not perform as expected. The migration completed successfully, and the workload entered a running state at the target site. However, workload behavior and/or user experience is incorrect due to various failure conditions. The cloud subscriber raises an incident to the cloud provider.

Failure Condition 4:
The cloud provider cannot meet the usage scenario goals without introducing unacceptable risks, such as network broadcast storms or network loops.
**Usage Scenario 3 – Disaster Recovery**

- **Motivation:** Business Continuity
- **Migration Class:** Relocate

According to *IT Infrastructure Library* (ITIL)*, continuity management is the process by which plans are put in place and managed to ensure that IT services can be recovered, and continue, should a serious incident occur. This includes, of course, both proactive and reactive measures to reduce the risk and impact of a disaster in the first place. This usage scenario focuses on measures to mitigate the effects of and recover from an incident after it has occurred. (Data loss may not be fully prevented by this usage scenario. Prevention is addressed in Usage Scenario 6, Disaster Avoidance.)

The “Disaster Recovery” usage scenario is in the Relocate class, and may employ at-rest or live migration, specifically:

**Phase 1:** The following steps would be performed periodically in preparation for a possible serious disruptive incident. The frequency of these updates will be according to the SLA between the cloud subscriber and cloud provider.

1. Construct a manifest of all workload components and requirements at the source site. This could be done by either the cloud subscriber or cloud provider, depending upon their contract and SLA. This manifest will be used in the orchestration of the remaining steps.
2. The cloud provider will deploy all required software applications and system components to the disaster recovery target site.
3. The cloud provider will replicate storage to the disaster recovery target site, again based on an agreed or specified schedule/frequency. This includes validation of complete and correct replication.

**Phase 2:** The next steps below would be performed in response to a disaster or other serious incident:

4. The application or workload is activated at the target, and set to receive connections.
5. The cloud provider redirects traffic to the disaster recovery target site, as per SLA with the cloud subscriber.
6. All QoS, performance, security, and availability characteristics at target must be at parity with the source, unless otherwise agreed by the cloud subscriber.
7. After the recovery of the damaged site (source), the workload is migrated back to the original location. The same steps as defined above have to be performed again, in the other direction, to recreate the disaster recovery site.

**Note:** Both success scenarios below are required for this usage scenario to be considered successful.

**Success Scenario 1:**
The workload is successfully migrated from the source to the target (Phase 1). Testing can be performed by the cloud subscriber to confirm readiness for potential source disruption.

**Success Scenario 2:**
After a disruption at the source site, the recovery site target comes online as planned and takes connections properly. Successful operations are delivered out of the target site (Phase 2).

**Failure Condition 1:**
The migration was interrupted or not possible (Phase 1). The migration did not complete successfully, and therefore the workload is unable to enter running state at the target. Return Error code is expected to allow for retry or failure event notice.

---

* http://www.itil-officialsite.com/
Failure Condition 2:
The migrated workload cannot be started and does not work as intended. The migration completed successfully. However, the workload is unable to enter running state due to various failure conditions (Phase 2). Return Error code is expected to allow for retry, or failure event notice.

Failure Condition 3:
The migrated workload does not perform as expected. The migration completed successfully, and the workload can enter a running state at the target site. However, workload behavior and/or user experience is incorrect due to various failure conditions. The cloud subscriber raises an incident.

Failure Condition 4:
The cloud provider cannot meet the usage scenario goals without introducing unacceptable risks, such as network broadcast storms or network loops.

**Usage Scenario 4 – Follow-The-Moon**

- **Motivation:** Resource Locality
- **Migration Class:** Extend

The Extend migration class can be employed for situations where there is a progressive or incremental affinity to physical resources. For example, consider follow-the-moon requirements, where workloads are migrated to data centers where power and cooling are cheapest, based on time of day.

Note that this usage scenario does not assume a hard cut-over from source to target. On the contrary, it assumes that business requirements dictate that the migration occurs over an extended period of time.

Below are the high-level steps for using the Extend migration class to implement follow-the-moon:

1. Construct a manifest of all workload components and requirements at the source site. This could be done by either the cloud subscriber or cloud provider, depending upon their contract and SLA. This manifest will be used in the orchestration of the remaining steps.
2. The cloud provider will deploy all required software applications and system components to the target site.
3. The cloud provider will replicate storage to the target site.
4. The cloud provider will execute a migration of the designated subset of workloads.
5. Once the migration is confirmed complete and correct, the cloud provider will add the target location to the load-balanced group, with rules reflecting the cloud subscriber’s business priorities for the source/target split.
6. All QoS, performance, security and availability characteristics at target must be at parity with the source, and be maintained at the source, unless otherwise agreed upon by the cloud subscriber.
7. Repeat steps 3 through 6 according to cloud subscriber requirements and schedule until all remaining required workloads have been migrated from the source to the target. This could occur over an extended period of time.

Note that steps 3 through 5 above should be treated as an atomic event. Migration failure during any of those steps should cause a full rollback and continuation to operate with the in-place resources.
USAGE SCENARIO VARIATION: LAZY FOLLOW-THE-SUN

A cloud subscriber may need to move content and capability close to users through the course of a 24-hour day, but there cannot be a hard cut-off to users remaining on the source site. This may be applicable to applications similar to content delivery, where optimum geographic location for cached content will change as Internet users gradually come online/offline throughout their day in their respective time zones. So, whereas follow-the-moon is an example of the Extend class for Resource locality requirements (see “Purpose” section), lazy follow-the-sun is also an instance of the Extend class, but driven by the follow-the-sun motivation.

Success Scenario 1:
The workload is added at target without interruption to workload execution, and without disruption to state at the source. Target is successfully added to the load-balance group.

Failure Condition 1:
The migration was interrupted or not possible. The migration did not complete successfully, and therefore the workload is unable to enter running state at the target. Roll back to the source site and Return Error code are expected to allow for retry or failure event notice.

Failure Condition 2:
The migrated workload cannot be started and does not work as intended. The migration completed successfully. However, the workload is unable to enter running state due to various failure conditions. Roll back to the source site and Return Error code are expected to allow for roll back and retry, or failure event notice.

Failure Condition 3:
The migrated workload does not perform as expected. The migration completed successfully, and the workload entered a running state at the target site. However, workload behavior and/or user experience is incorrect due to various failure conditions. The cloud subscriber raises an incident to the cloud provider.

Failure Condition 4:
The cloud provider cannot meet the usage scenario goals without introducing unacceptable risks, such as network broadcast storms or network loops.

USAGE SCENARIO 5 – CLOUD BURSTING

- **Motivation:** Dynamic Scaling
- **Migration Class:** Extend

Usage Scenario 5 is motivated by a cloud subscriber’s requirement to dynamically scale its capacity, and is in the Extend migration class. While it’s considered part of migration, it involves adding workload capacity, not strictly moving workloads. The Extend migration class requires a shift in thinking towards the idea of running workloads across multiple data center sites as a single horizontally scalable capability. The application’s architecture should follow the recommendations noted in the ODCA Whitepaper *Developing Cloud-Capable Applications*.

Below are the high-level steps for using the Extend migration class to implement cloud-bursting:

1. Construct a manifest of all workload components and requirements at the source site. This could be done by either the cloud subscriber or cloud provider, depending upon their contract and SLA. This manifest will be used in the orchestration of the remaining steps, below.
2. The cloud provider will deploy all required software applications and system components to the target site.
3. The cloud provider may replicate storage to the target site (alternatively the data repository can remain in place).
4. The cloud provider will instantiate the additional workload at the target site.
5. Once the live migration is confirmed complete and correct, the cloud provider will add the target location to the load-balanced group.

6. All QoS, performance, security, and availability characteristics at the target must be at parity with the source, and be maintained at the source, unless otherwise agreed by the cloud subscriber.

Note that steps 3 through 5 above should be treated as an atomic event. Migration failure during any of those steps should cause a full roll back and continuation to operate with the in-place resources.

Application components, reference data, or other components may be pre-positioned in advance of the migration event.

**USAGE SCENARIO VARIATION: FRANCHISE DEPLOYMENT**

The Extend migration class could also be employed for situations where a business is growing, and needs to add workload capacity and capability, but in a less dynamic fashion. Consider a large business setting up new retail storefronts or a hospital network setting up outlying member clinics. In this case, workloads and associated capacities are set up according to the creation or deployment of said business unit. Dynamic scaling between the central organization and smaller office is not a driver.

**USAGE SCENARIO VARIATION: ELASTIC LOAD BALANCING**

Note this could also be adapted for elastic or dynamic load balancing, where workload traffic is distributed throughout multiple application instances with the further ability to automatically add capacity based on defined policies or thresholds.

**Success Scenario 1:**
The workload is successfully added to the target without disruption to state at the source. The target is successfully added to the load-balance group.

**Failure Condition 1:**
The addition was interrupted or not possible. The addition did not complete successfully, and therefore the workload is unable to enter running state at the target. Roll back to the source site and Return Error code are expected to allow for retry or failure event notice.

**Failure Condition 2:**
The added workload cannot be started and does not work as intended. The addition completed successfully. However, the workload is unable to enter running state due to various failure conditions. Roll back and Return Error code are expected to allow for roll back and retry or failure event notice.

**Failure Condition 3:**
The added workload does not perform as expected. The addition completed successfully, and the workload entered a running state at the target site. However, workload behavior and/or user experience is incorrect due to various failure conditions. The cloud subscriber raises an incident to the cloud provider.

**Failure Condition 4:**
The cloud provider cannot meet the usage scenario goals without introducing unacceptable risks, such as network broadcast storms or network loops.
USAGE SCENARIO 6 – DISASTER AVOIDANCE

- Motivation: Business Continuity
- Migration Class: Sustain

According to ITIL®, continuity management is the process by which plans are put in place and managed to ensure that IT services can be recovered and continue without data loss should a serious incident occur. This includes, of course, both proactive and reactive measures to reduce the risk and impact of a disaster in the first place. This usage scenario focuses on measures to prevent a service interruption from a disaster.

For the cloud, disaster avoidance requires moving workloads over to another site in advance of a disaster without having to incur downtime.

The disaster avoidance usage scenario is in the Sustain migration class, and necessitates live migration, specifically:

1. Construct a manifest of all workload components and requirements at the source site. This could be done by either the cloud subscriber or cloud provider, depending upon their contract and SLA. This manifest will be used in the orchestration of the remaining steps.
2. The cloud provider will deploy all required software applications and system components to the disaster recovery target site. Ideally some or all of this could be pre-staged before an incident, but this is not typically necessary.
3. The cloud provider will migrate storage and/or data to the disaster recovery target site.
4. Once storage migration is complete and correct, the cloud provider will execute a live-migration event on the virtual machines.
5. Once the live-migration is confirmed complete and correct, the cloud provider will redirect traffic to the disaster recovery target site.
6. All QoS, performance, security, and availability characteristics at the target must be at parity with the source, unless otherwise agreed upon by the cloud subscriber.
7. After some time the decision must be taken regarding whether the workload should move back to the source site.

Note that steps 3 through 5 above should be treated as an atomic event. Migration failure during any of those steps should cause a full roll back to the source site.

USAGE SCENARIO VARIATION: DATA CENTER CLOSURE

The Sustain migration class could also be employed for less critical situations where a second site needs to be a replica or replacement of an original, such as a data center move. Migrating workloads from a source site to a target in a controlled manner could significantly ease the logistical burden of transitioning or closing a data center.

Success Scenario 1:
The workload is migrated from the source to the target without interruption to workload execution and without disruption to state. Control and traffic are successfully set to the target.

Failure Condition 1:
The migration was interrupted or not possible. The migration did not complete successfully, and therefore the workload is unable to enter running state at the target. Roll back to the source site and Return Error code are expected to allow for retry or failure event notice.

Failure Condition 2:
The migrated workload cannot be started and does not work as intended. The migration completed successfully. However, the workload is unable to enter running state due to various failure conditions. Roll back to the source site and Return Error code are expected to allow for roll back and retry or failure event notice.
Failure Condition 3:
The migrated workload does not perform as expected. The migration completed successfully, and the workload entered a running state at the target site. However, workload behavior and/or user experience is incorrect due to various failure conditions. The cloud subscriber raises an incident to roll back to the source site.

Failure Condition 4:
The cloud provider cannot meet the usage scenario goals without introducing unacceptable risks, such as network broadcast storms or network loops.

SERVICE TIERS

The features below are generally applicable to both IaaS and PaaS, and are derived from the ODCA Standard Units of Measure. For this Usage Model, it is not intended that all of the features in a given column below must all be supported as a group. In practice, a given service provider solution will combine different service levels for different elements. For example, Gold Security features may be combined with Bronze Performance features.

It is the cloud provider’s responsibility to differentiate service tiers within a given data center or service offering.

<table>
<thead>
<tr>
<th>Security</th>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
<th>Platinum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Enterprise equivalent</td>
<td>Critical market or business sector equivalent</td>
<td>Military or safety-critical equivalent</td>
<td></td>
</tr>
<tr>
<td>As per ODCA Provider Assurance Usage Model 11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Effectiveness</td>
<td>98% migration success rate</td>
<td>99% migration success rate</td>
<td>&gt;= 99.9% migration success rate</td>
<td>&gt;=99.99% migration success rate</td>
</tr>
<tr>
<td>General Performance</td>
<td>Migration configured in correct manner</td>
<td>Migration tuned to the components and workloads in question. Performance is monitored and significant deviations remedied.</td>
<td>Additional measures applied to sustain acceptable migration speed. Performance monitored, service penalties applicable.</td>
<td>End-user experience monitored, significantly increased service penalties for failure / degradation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Bronze</th>
<th>Bronze</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-Provider Migration</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports Cost-Sensitive Migration</td>
<td>No</td>
<td>Select migration choices at different pricing levels.</td>
<td>Enhanced migration choices with customer selectable options. &quot;A la carte&quot; migration choices.</td>
<td>Support for automated cost-function driven migration planning and scheduling&lt;sup&gt;12&lt;/sup&gt;.</td>
</tr>
<tr>
<td>Client SLA Priority</td>
<td>Reasonable efforts to respond to client needs, but lowest priority.</td>
<td>Provisions made to provide a good service and be responsive to the client, attentive to problems, with documented and consistent response and recovery times, and so on.</td>
<td>Enhanced service level, providing priority attention for all incidents, service interruptions, phone calls. Penalties for failure to deliver.</td>
<td>First priority access to resources on any incident. Dedicated team for highest level of reporting and interfacing. Major service penalties for breach.</td>
</tr>
<tr>
<td>Recovery Time Objective (for DA and DR)</td>
<td>48 hours</td>
<td>8 hours</td>
<td>2 hours</td>
<td>10 minutes</td>
</tr>
<tr>
<td>Supports At-Rest Migration</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports Live Migration</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Live Migration Performance</td>
<td>N/A</td>
<td>Can migrate live workloads with &lt; 100% workload slow-down during migration, i.e., the workload may take up to twice as long to execute.</td>
<td>Can migrate live workloads with &lt; 50% workload slow-down during migration.</td>
<td>Can migrate live workloads with &lt; 20% workload slow-down during migration.</td>
</tr>
<tr>
<td>Live Migration Distance</td>
<td>20km or greater between sites, or 40ms or greater latency (one-way).</td>
<td>100km or greater between sites, or 40ms or greater one-way latency</td>
<td>100km or more between sites or 40ms or greater one-way latency.</td>
<td>100km or more between sites or 40ms or greater one-way latency.</td>
</tr>
<tr>
<td>Supports Concurrent Migration</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>


**Note:** Latency times above are deliberately conservative. Actual observed between data centers may be significantly better.
RFP REQUIREMENTS — SOLUTION PROVIDERS
Following are requirements that the Alliance believes should be included in requests for proposal to cloud providers to confirm that proposed solutions support long distance workload migrations.

ODCA Principle Requirement - Solution is open, works on multiple virtual infrastructure platforms, and is standards-based. Describe how the solution meets this principle and any limitations towards the ODCA principle.

ODCA Long Distance Migration Usage Model 1.0 — Solution should support all of the following:
- Compliance with ODCA VM Interoperability Usage Model¹³, including import and export of VM packages per OVF.
- Export / import / create workloads with the defined configurations.
- Copy workloads with data from source to destination.
- Copy data incrementally in a differential mode for large volumes of data (e.g., copy changes only).
- The ability to synchronize the source and the target.
- Transmit the data from storage/virtual disk through OSI Layer 3 TCP or higher.
- Ability to change VM settings on the fly without starting the OS at the destination site (e.g., Change IP and hostname to prevent IP conflicts in the same network).

RFP REQUIREMENTS — SERVICE PROVIDERS
Following are requirements that the Alliance believes should be included in requests for proposal to cloud providers to ensure that proposed services support long distance workload migrations.

ODCA Principle Requirement - Service is open and is standards-based. Describe how the service meets this principle and any limitations towards the ODCA principle.

ODCA Long Distance Migration Usage Model 1.0 — For disaster avoidance and other live migrations, the service can move a workload to target without interruption to workload execution and without disruption to state.

ODCA Long Distance Migration Usage Model 1.0 — For all migration types, after a migration, user / session connections are successfully directed to the target as specified.

ODCA Long Distance Migration Usage Model 1.0 — For disaster recovery and other at-rest migrations, the workload is successfully migrated from the source to the target. Tests can be performed to confirm.

ODCA Long Distance Migration Usage Model 1.0 — For disaster recovery-motivated migrations, the recovery site target comes online as planned and takes connections properly. Successful operations are delivered out of the target site.

ODCA Long Distance Migration Usage Model 1.0 — For cloud bursting and other capacity-growth situations, the workload is added at target without interruption to workload execution and without disruption to state at the source. Target is successfully added to the load-balance group.

¹³ www.opendatacenteralliance.org/docs/ODCA_VMInteroperability_Rev.1.1_Final.pdf
ODCA Long Distance Migration Usage Model 1.0 – Service must provide the following orchestration capabilities:

- Check actual status (e.g., running versus not running).
- Stop / Start workloads.
- Workflow and dependency management.
- Start copy process with different characteristics, such as one time, differential mode-based on blocks/files.
- Pause/resume whole process or specific steps.
- The ability to test or simulate migrations, such as in an isolated network.
- Granular visibility to the cloud subscriber of migration processes and events.
- Roll back to the original state and site in the event of migration failure.
- Full automation throughout the orchestration process.
- Ability to define atomic steps in the migration workflow.
- Full support for policies specified and controlled by the cloud subscriber. For example, jurisdictional rules about data residency or rules about when workloads may not be disturbed.
- Support for multiple migrations, potentially concurrent, with different priorities and policies.
- All migrations should cause events that would go into a (security) log management tool.

ODCA Long Distance Migration Usage Model 1.0 – Service should also support the ability to create multi-provider management consoles for services supporting inter-provider migration. (This could take the form of standard APIs to integrate disparate providers.)

ODCA Long Distance Migration Usage Model 1.0 – Service should also support the ability to cope with workload migrations between non-identical infrastructures. For example, could a workload manifest include conditional logic to account for different target site security or features?

Click [here](https://www.opendatacenteralliance.org/ourwork/proposalengineassistant) for an online assistant, Proposed Engine Assistant Tool (PEAT) to help you detail your RFP requirements.

SUMMARY OF INDUSTRY ACTIONS REQUIRED

In the interest of giving guidance on how to create and deploy solutions that are open, multi-vendor and interoperable, the Alliance has identified specific areas where it believes there should be open specifications, formal or de facto standards, or common IP-free implementations. Where the Alliance has a specific recommendation on the specification, standard, or open implementation, it is called out in this usage model. In other cases, we will work with industry to evaluate and recommend specifications in future releases of this document.

Successful implementation of long-distance migration will be dependent upon good orchestration solutions, which are preferably standardized among cloud providers. The following are next steps and industry actions required to refine and implement this usage model:

1. ODCA needs to engage with other bodies (providers and vendors) to identify and endorse migration orchestration standards, compatible with and extending the [ODCA VM Interoperability Usage Model](https://www.opendatacenteralliance.org/docs/ODCA_SecurityMonitoring_Rev1.1_Final.pdf). This should address migration of workloads between disparate cloud providers.

2. ODCA needs to engage with other bodies to create an industry-wide agreed-upon abstraction of a PaaS workload.

3. Solution providers need to propose solutions to minimize the amount of data to be transferred at the time of migration.

---


15 [www.opendatacenteralliance.org/ourwork/proposalengineassistant](https://www.opendatacenteralliance.org/ourwork/proposalengineassistant)
4. Solution providers need to propose solutions that implement this usage model, including consistent methods for initiating migrations, target site resources and capabilities, migration prioritization, and so on.

5. Solution providers should provide their application stacks according to the ODCA Whitepaper *Developing Cloud-Capable Applications*.

6. Solution providers should conduct testing and demonstrations on how long distance workload mobility is achieved while minimizing traffic tromboning.