Operational Policy and Transparency for IaaS

Enterprise Cloud Customer Council Technical Working Group Position Paper

December 2016

Preamble

Overview

The Enterprise Cloud Customer Council (E3C) is a group of enterprise companies, primarily financial services, with the vision to become a leading voice for enterprise organizations in the pursuit of cloud interoperability, security, and portability with major cloud industry vendors and standards bodies. The top cloud companies are closely involved and are actively assisting the E3C in achieving its goals. Intel Corporation serves as facilitator for the group.

Mission

The E3C mission is to develop requirements centered on common functional architecture, detailed specifications, and technical solutions that improve enterprise cloud adoption and integration while mitigating regulatory risk.

For the smooth and secure usage of hybrid cloud for applications and data, the council shall work toward

1) Enhancing security of clouds for secure network connectivity and data management that align to enterprise requirements
2) Ease of integration and life cycle management through interoperability across clouds
3) Ensuring enterprises have the same visibility and control of their resources in public cloud as on premises

Process

In order to achieve the E3C mission, the members form technical work groups focused on the top current impediments. The technical work groups work towards understanding common architectures and approaches and then establishing common requirements that form the E3C position papers. After the papers are approved by the E3C council members, consisting of executive level members from each of the member companies, the papers are published on a public website. Papers will be iterated accordingly as needed.

Usage of Position Papers

The position papers are not designed as prescriptive requirements but rather as input for organizations developing roadmaps and/or requirements relating to cloud adoption. These are freely available, however please reference E3C if you utilize these in RFPs, RFQs, publications, etc.

Document Conventions

RFC 2119 conventions apply to this document. For convenience, these definitions are provided here:

1. MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. MUST NOT: This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3. SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

5. MAY: This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

Overview

This position paper focuses on a number of operational and transparency concerns around Infrastructure as a Service within Cloud Service Providers, specifically virtual machines and related resources. This paper is not an exhaustive list of positions or requirements in this space, but will focus on select topics including instance availability, maintenance windows, live migration, and audit logging.

1. Maintenance and Instance Availability

Customers need the ability to influence when planned activities can be scheduled for the instances and core infrastructure components running on the public cloud, based on their application deployment's risk profile and resiliency characteristics. Therefore, a method is required to explicitly signal when planned maintenance is scheduled, with the ability to define time-to-live or other constraints (maintenance windows) for specific operations like restarting or live-migrating instances.

1. Planned CSP initiated events that might disrupt VM instance availability must be scheduled during a maintenance window.
    a) CSP initiated events impacting instance availability may include hypervisor upgrades, configuration changes, hardware replacement, instance placement optimizations, networking changes, etc.
    b) Short-lived instance types without availability or with reduced availability guarantees are not in scope for this requirement.

2. Maintenance windows for planned CSP initiated events should be customer configurable.
    a) Customers should have the option to force immediate maintenance or defer maintenance to the next window, as long as it occurs before a final date or window.
    b) Maintenance windows may be defined as a set of hours on specific days of the week.

3. Unplanned CSP events must follow a CSP documented and deterministic process. These events should only encompass critical security-related remediation, resolution of unexpected hardware failures, and events subject to force majeure.

4. All maintenance policies, actions, and notifications, must be API-driven.

5. Instances that are part of the same application deployment or family should have maintenance events interspersed within, and when possible across, maintenance windows to reduce potential application impact or downtime.
    a) Development or test instances within an application may be flagged by the customer to receive updates before other instances.

6. Maintenance events on single-tenant shared infrastructure services that may impact or cause downtime for multiple instances must have a CSP defined notification period.
    a) Single-tenant shared infrastructure services may include but are not limited to virtual networks, hybrid network interconnection, and related security policies.

2. Live Migration

Live migration refers to the process of moving a running virtual machine instance between different physical machines, including memory, storage, and network connectivity, without application interruption or disconnecting clients. Some applications within financial services are sensitive to live migration operations, including trading applications with clock synchronization tolerance requirements on the order of milliseconds as required by FINA 16-23 [1] and SEC Rule 613 [2].

1. Live migration must be configurable as an enable/disable policy for virtual machine instances.

2. By default, live migration events may be executed at any time. However, customers should have the ability to define maintenance window constraints on live migration events.
    a) Using an example of a time-sensitive trading application, it may be okay to live migrate the application during a scheduled maintenance window outside of business/market hours, but not okay during market hours.

3. If live migration is disabled for an instance, maintenance events may require instance downtime. In this scenario, the recovery behavior of the instance must be configurable.
    a) The customer should define a default action (e.g. restart, stop, or terminate instance) to execute to satisfy maintenance events.
    b) The customer may manually opt-in to live migrate an instance to satisfy a maintenance event before the default action is executed.

4. The transfer of running memory and other instance state during a live migration event must occur over an encrypted transport.

5. Live migration events must be logged to the CSP's auditing/logging system and exposed to the customer. The log should include metrics on the instance's blackout and brownout times during the live migration, as well as the reason for the live migration.

6. The CSP should provide customers a live migration blackout time SLO and document potential application impact during live migration (e.g. network packet loss).

[1] http://www.finra.org/industry/notices/16-23
[2] https://www.sec.gov/divisions/marketreg/rule613-info.htm

3. Transparency and Telemetry

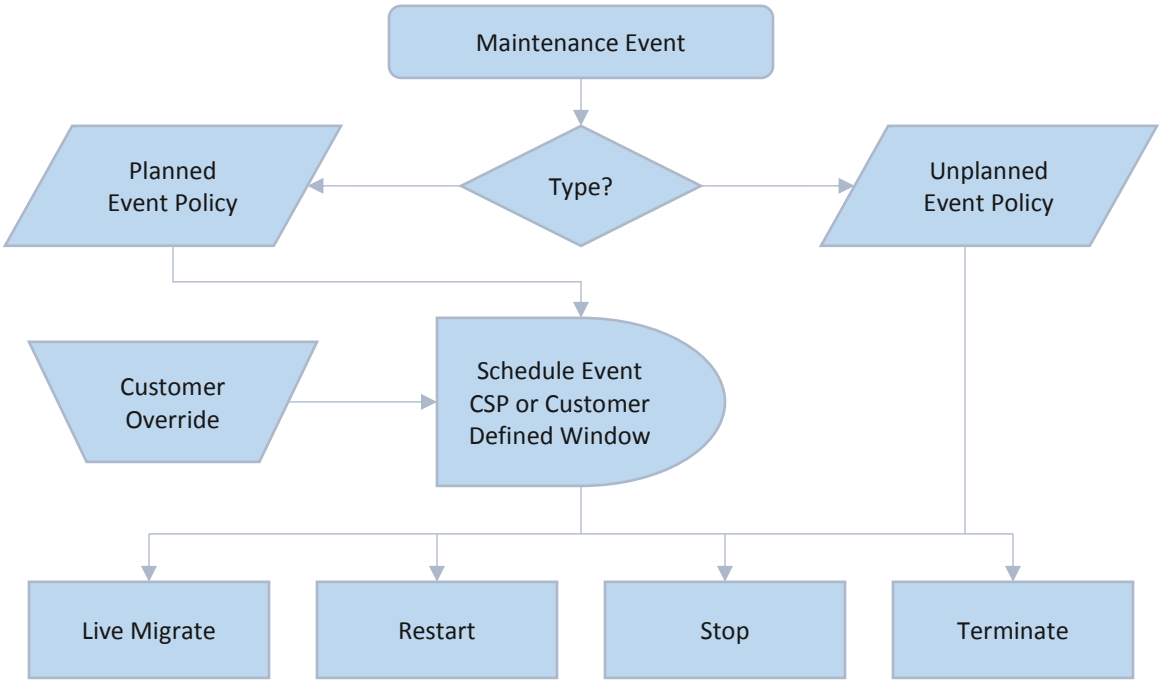
1. All actions executed within a customer's account must be logged to an immutable audit logging service.
    a) The audit log should be retained for a customer-defined period of time.
    b) Audit log timestamps should be in UTC or include a UTC time zone offset (e.g. ISO 8601).
    c) The log stream should expose events on a near real-time basis and be accessible via an API in a machine-readable format (e.g. JSON).
    d) The log data should be encrypted and may be encrypted by a provider-generated and managed encryption key.

2. All activities, events, or incidents that adversely impact the availability, performance, or security of the customer's resources must be logged and exposed to the customer. Security incident and vulnerability disclosure must follow a documented and industry standard process.

3. All CSP administrative access to runtime systems must be audited, constrained, just in time, and not be required for the steady state operation of the CSP environment.

4. All CSP administrative access to a customer's account or resources must be audited and exposed to the customer. Access to modify a customer's resources or read/write customer data must be pre-approved by the customer – this may need to occur as part of a support case or troubleshooting.

4. Policy Examples



1. FX Trading Application
   - Instances: 2 Always On
   - Maintenance Window: Saturday or Sunday, 12am – 12pm
   - Live Migration
     - In Window: Enabled
     - Out of Window: Disabled
   - Recovery Behavior
     - In Window: Auto-Restart Instance
     - Out of Window: Stop Instance

2. Intranet Web Application
   - Instances: Autoscaling Group (Min 2, Max 10)
   - Maintenance Window: Every Day, 8pm – 10pm
   - Live Migration: Enabled
   - Recovery Behavior: Auto-Restart