

sdnp discussion group  
Internet Draft  
Intended Status: Informational  
Expires: April 21, 2012

D. McDysan  
Verizon

October 24, 2011

## Cloud Bursting Use Case

draft-mcdysan-sdnp-cloudbursting-usecase-00.txt

### Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at  
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on April 17, 2011.

### Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Abstract

This draft describes a use case for the overall coordination, control and management of "cloud bursting" in a hybrid cloud computing environment involving a private data center and a public or virtual private multi-tenant data center. This use case may be relevant to the Software Driven Network Protocol [SDN\_UC], VPN for Data Center [VPN4DC], or Cross Stratum Optimization [CSO] discussions in the IETF.

## Table of Contents

1. Introduction.....	2
2. Conventions used in this document.....	2
2.1. Acronyms.....	2
2.2. Terminology.....	3
3. Motivation and Background.....	3
4. Proposed Use Case.....	3
4.1. General Dynamic Cloud Computing Functionality.....	3
4.2. Private Data Center Use Case Elements.....	5
4.3. Public of Virtual Private Data Center Elements.....	6
5. Security Considerations.....	7
6. IANA Considerations.....	7
7. References.....	7
7.1. Normative References.....	7
7.2. Informative References.....	7
8. Acknowledgments.....	8

## 1. Introduction

This draft describes the cloud bursting use case for implementing dynamic cloud computing in a multi-tenant environment that addresses the case where computing, storage, application, security, networking resources are dynamically assigned.

Section 3 provides some motivation and background for the cloud bursting use case. Section 4 provides more details on the cloud bursting use case.

The draft cites a number of references that provide further detail on specific aspects of the use case and/or requirements.

## 2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [RFC2119].

### 2.1. Acronyms

SDNP	Software Driven Network Protocol
VPN4DC	VPN for Data Center
CSO	Cross Stratum Optimization

## 2.2. Terminology

Private Cloud - operated by an enterprise

Public Cloud - multitenant data center operated by a service provider accessed via the "Public" Internet

Virtual Private Cloud - multitenant data center operated by a service provider accessed via a L2 and/or L3 Virtual Private Network (VPN)

Hybrid Cloud - Dynamically instantiated instance of a public or virtual private cloud to (temporarily) augment capacity of a private cloud

## 3. Motivation and Background

Currently, mostly static L1/L2/L3 networks interconnect customer applications in Private Enterprise data centers. Note that an Enterprise application network may also contain sites that support sensor data collection and other forms of input or output. In order to provide capacity in support of dynamic application demand from Enterprises, cloud service providers are deploying virtualized resources (e.g., processing, storage, apps/OS) in Cloud Computing Centers.

Some dynamic bandwidth on demand being done in access networks, but this is often not automatically coordinated with networking in a cloud data center. Furthermore, assignment, reservation and configuration of other resources needed by the application, such as computing, storage, access to databases, or specific software instances is not well coordinated with the assignment of network capacity. An opportunity exists to standardize methods to optimize the assignment of L1, L2, L3 network capacity, Cloud Computing site selection and/or resource allocation more dynamically.

Such an optimization may be done proactively on a reservation basis, reactively in response to ad hoc requests, reactively in response to detected changes in load using pre-defined policies, or reactively by the provider in response to an aggregate of a number of smaller requests and/or reservations in order to make the system more efficient, and/or prepare for honoring a future reservation.

## 4. Proposed Use Case

This draft describes a use case for the overall coordination, control and management of "cloud bursting" in a hybrid cloud computing environment involving a private data center and a public or virtual private multi-tenant data center. This use case describes more details for a similar use case described in section 6.2 of [SDN\_UC], section 3 of [CSO] or [VPN4DC].

### 4.1. General Dynamic Cloud Computing Functionality

A cloud computing instance requires control and management at least the following. Further details on use cases and requirements are listed as references for many of the items below.

- o .Layer 2/Layer 3 bandwidth configuration and monitoring (scheduler weight setting, policer setting, reserving bandwidth (e.g., MS-PW), counter collection)
- o .VPN membership (e.g., VLAN, PBB, L2VPN/L3VPN), reachability and any restrictions on communication within the VPN [VPN4DC], [VROM]
- o .Compute resource allocation: virtual machines, virtual memory, OS, software assignment and activation on a physical computer [VROM]
- o .Storage resources: Partition(s) (e.g., Logical Unit Name (LUN)) assigned to physical storage [VROM]

There may also be a need to configure the following to align with the above

- o Firewall rules (e.g., ACLs) and other settings [FWLBDC]
- o Load balancers and settings [FWLBDC]
- o Security functions (encryption) [VDC\_SEC], [DVNSEC]
- o Network Address Translation (NAT) settings [DVN\_SEC]
- o Dynamic IP and/or L2 address mobility support

Furthermore, the request may also have performance related parameters, such as [CSO]

- o Packet transfer performance between sites (e.g., latency, delay variation, loss)
- o Availability and failure recovery time objectives for classes of resources (e.g., percentage up time and time to recover from an interface failure)
- o Diversity or fate sharing avoidance constraints (e.g., sets of cloud resources are placed in sites that do not share fate for failure events)

A Private Cloud Enterprise customer desires a single unified method to invoke all of the above aspects of a hybrid cloud service in a transaction such that either all aspects are instantiated, or if any aspect cannot be instantiated then the overall transaction will either fail or result in the next step in a capability/performance negotiation. Previously, this unified methods has been called a "Northbound API," and more recently an "Application-to-Orchestrator protocol" [SDN\_PS]. In some cases, a negotiation could occur where the SDN system responds with a capability and/or performance indication that is "closest" to what was requested as a next step in a negotiation process. The Enterprise customer could then have the option to accept this offer, or make another request with changed parameters.

A higher-level system could use interfaces (many of them already standardized by the IETF or other SDOs) to implement the above

control/management interfaces to accomplish this objective as illustrated in Figure 1. The SDN controller could be viewed as implementing a set of "plug-ins" [SDN\_PS] for controlling the management, control and/or data plane of the various devices listed above (a subset being illustrated in Figure 1).

Alternatively, signaling between some of these elements for implementing some functions and state/configuration communication could be employed, for example, as described in [VPN4DC].

Furthermore, not all of these interfaces need be standardized in all cases. For example, the private cloud site(s) could have its own controller and the cloud provider another controller. The required interaction is then between these data center controllers and the interfaces within the private cloud need not be standardized.

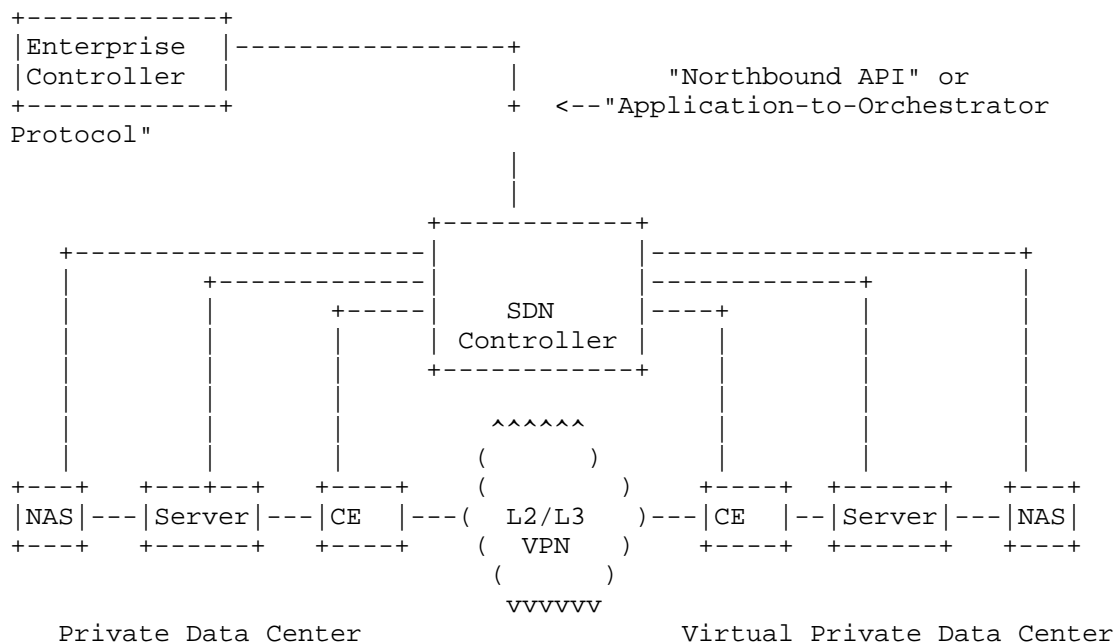


Figure 1 Hybrid Cloud Bursting Use Case Context

#### 4.2. Private Data Center Use Case Elements

Private Data Center controller (may be automated, or a combination of manual and automatic actions) requests the following at one or more private Cloud sites:

- o Configure VM assignment/movement within private cloud
- o Configure storage, LUN assignment/movement within private cloud
- o Configure private cloud switch/router access to networking (e.g., scheduler weights, policer, enable specific L2/L3 addresses)

- o Configuration of any VPN reachability and the requested components from the cloud service provider within the private cloud sites
- o Private cloud Load Balancer, NAT settings
- o Private cloud Firewall, Security function settings
- o Configuration needed to meet performance objectives and/or constraints in Private Cloud Elements.

Usually, the Enterprise operator of the private data center would do all of the above. However, a service provider could do settings for some components. For example, setting the scheduler weights on the switch/router that interfaces to the L2/L3 VPN or Internet access could be done via the service provider.

#### 4.3. Public of Virtual Private Data Center Elements

The SDN controller function of Figure 1 accepts a "Northbound API" request from an Enterprise controller and performs following actions at one or more cloud provider Virtual Private or Public cloud sites.

- o .Configure VM assignment/movement within the Enterprise and provider data center(s). Note that this may require usage of the same or compatible hypervisors with appropriate communication and/or permissions between the hypervisor controllers.
- o .Configure storage, LUN assignment/movement within the provider data center(s). Note that this may require usage of the same or compatible network attached storage systems with appropriate communication and/or permissions between the storage controllers.
- o .Configure bandwidth related characteristics of L2/L3 packet network (e.g., bandwidth for an MS-PW, additional (logical) ports, scheduler weights, policers, addresses). This includes logical connectivity between and enterprise and a provide cloud site as well as between enterprise sites, and between provider cloud sites.
- o .Configure VPN-related characteristics within public or virtual private data center (e.g., mapping to L2/L3 VPN service, firewall)
  - o This may include further definitions of reachability within the L2/L3 VPN or the notion of a Virtual Data Center. See [VPN4DC].
- o .Configure access to networking (e.g., scheduler weights, policer, enable specific L2/L3 addresses) on the Public Virtual Private data center switches or routers
- o Virtual, multi-tenant Private Firewall and security function settings
- o Virtual, multi-tenant Private Load balancer and NAT settings

- o Configuration needed to meet performance objectives and/or constraints. In some cases, the service provider may need to propose an alternative to progress a negotiation if not all objectives or constraints can simultaneously be met. Furthermore, the SDN controller must perform composition across all Enterprise private cloud sites and candidate public or virtual private cloud sites to ensure that the requested performance objectives are delivered.

Usually, the service provider of the public or virtual private cloud data center would do all of the above.

## 5. Security Considerations

A number of virtual data center security requirements and gaps are described in [VDC\_SEC] and [DVN\_SEC]. This draft addresses some of these requirements as follows.

Consistent, automatic configuration of VPN membership in the private and public/virtual private cloud is necessary to provide isolation between customers.

Consistent, automatic configuration of firewalls in the private and public/virtual private cloud is necessary to provide fine-grained access control for various virtual data center resources.

Consistent, automatic configuration of security functions (e.g., encryption, authentication, intrusion detection, etc.) in the private and public/virtual private cloud is necessary to provide confidentiality, non-repudiation, and authentication for various virtual data center resources.

## 6. IANA Considerations

None

## 7. References

### 7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

### 7.2. Informative References

[SDN\_UC] Ping Pan, Tom Nadeau, "Software-Defined Network (SDN) Problem Statement and Use Cases for Data Center Applications," Work in Progress

[SDN\_PS] Tom Nadeau, "Software Driven Networks Problem Statement," Work in Progress.

[VPN4DC] Ning So et al, "Requirements of Layer 3 Virtual Private Network for Data Centers," work in progress.

[CS0] Greg Bernstein, Young Lee, "Cross Stratum Optimization Use-cases," work in progress.

[CLO] Young Lee et al, "Problem Statement for Cross-Layer Optimization," work in progress.

[VROM] V. Grado, T. Tsou, N. So, "Virtual Resource Operations & Management in the Data Center," work in progress

[FWLBDC] Y. Gu, Y.Fan, "Policies and dynamic information migration in DCs," work in progress

[VDC\_SEC] S. Karavetttil et al, "Security Framework for Virtualized Data Center Services," work in progress

[DVN\_SEC] M. Ko, E. Wang, "Problem Statement for Setting Up Dynamic Virtual Network," work in progress

## 8. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Copyright (c) 2011 IETF Trust and the persons identified as authors of the code. All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This code was derived from IETF RFC [insert RFC number]. Please reproduce this note if possible.

## Authors' Addresses

Dave McDysan  
Verizon  
22001 Loudoun County PKWY  
Ashburn, VA 20147  
Email: dave.mcdysan@verizon.com



