Using Layer 7’s API Gateway for vCloud Architectures

How to achieve abstraction, security and management of vCloud APIs

White Paper
Executive Summary
Layer 7 Technologies has partnered with VMware to provide a solution for securing and managing the vCloud API hosted by Virtual Cloud Director (vCD). This document describes an architecture that incorporates Layer 7’s CloudSpan CloudControl gateway to provide cloud API security and management of the vCloud API published in a vCD instance. This API may be used by either the customer-base of the vCD cloud, or by vCD administrators.

The CloudControl API Gateway enables decoupling of common aspects of security and management from APIs into a dedicated API Gateway that can be deployed as a virtual application appliance in the vCloud platform. The use of an API Gateway in front of the vCD APIs promotes consistent application of access, security and SLA policies across all vCD APIs plus accurate lifecycle management and governance of the APIs themselves. CloudControl sits as a proxy between the vCD APIs and the consumers of those APIs and provides a layer of abstraction, mediation and control between the API users and providers simplifying management for the API publisher.

This whitepaper is intended for vCloud operators. It introduces the concept of a vCloud API Gateway by looking at the functional and operational advantages of implementing a vCloud API architecture alongside vCloud APIs. This whitepaper then goes on to describe how the Layer 7 API Gateway can be used to meet the specific architectural specifications outlined in the vCloud Architecture Toolkit (vCAT).

Why Use an API Gateway with vCloud?
Introduction
The CloudSpan CloudControl API Gateway from Layer 7 Technologies simplifies how telcos, SaaS, PaaS, IaaS and enterprise service providers expose their provisioning, application, and data APIs to external partners, large customers, white label resellers and value-added developers. In many instances, these service providers must expose a combination of their own APIs and the underlying APIs of the cloud platform their infrastructure is built upon, such as VMware’s vCloud Director. This creates a need for a unified control, security and adaptation layer that can expose new interfaces without touching core application and data systems.

Layer 7’s CloudControl Gateway meets the needs of the service provider by providing both functional and operational benefits:

- Functional benefits increase the security, performance or capabilities provided by existing APIs
- Operational benefits make new and existing APIs easier to manage, version, and monitor

An API Gateway’s Functional Benefits for vCloud APIs
Layer 7’s CloudSpan CloudControl API Gateway increases the value of exposed data, provisioning and application APIs while maintaining the security necessary to prevent compromise of the services exposed via those APIs. These features include:
• Enforcement of sophisticated access control policies using existing Identity and Access Management (IAM) products, standards and credential mechanisms
• Confidentiality, integrity, and threat protection for incoming and outgoing application data.
• Transformation of message formats, transport protocols, and interface types
• Routing of content to appropriate endpoints based on requestor, content or availability
• Orchestration, re-composition and virtualization of service APIs to create value-added APIs
• Customized caching of calls to APIs, IAM servers, databases and other systems of record
• SLA management and metering of incoming requests to conform to policy-defined traffic preferences

**API Access Control**

API access control is dependent upon the authentication and authorization of incoming client credentials and message content against policies that make use of existing identity management solutions. Incoming credentials come in many forms, including username/password, x.509 digital certificates, Kerberos tickets, SAML assertions, OAuth tokens, or proprietary SSO tokens. CloudControl can accept any of these formats from a variety of sources and authenticate using almost any IAM solution, such as generic LDAP, Microsoft Active Directory, Tivoli Access Manager, Oracle Access Manager, Novell Access Manager, Sun OpenSSO, CA SiteMinder Policy Server, RSA ClearTrust or custom database authentication mechanisms. Authorization for the user, role, group or custom attribute can then use the same system, or can employ standards such as XACML, SAML assertion validation, or OAuth token validation. CloudControl connects natively with PKI systems, including support for CRLs, OCSP and DoD PKI integration, and provides a fully compliant WS-Trust Security Token Service (STS) within the Gateway. The STS is customizable to support the generation of new token types, allowing federation of identities between external and internal domains.

**API Data Confidentiality & Integrity**

CloudControl maintains the confidentiality and integrity of data transmitted to and from endpoint APIs. Starting at the network layer, transport security is provided through SSL (with user-specified constraints on acceptable cipher suites including newer ciphers such as elliptical curve cryptography) and IP whitelisting/blacklisting. Message-level security is provided using standards for encryption and digital signing of all or part of the content. Application-aware validation of XML schemas, HTTP headers, URL parameters, JSON data structures, and arbitrary content models provide an immediate rejection of any content that does not match the expected input patterns, and threat protection is provided for a broad range of application-level threats such as cross-site scripting, SQL injection, XML content threats, XML structural threats, and virus scanning of message contents and attachments.

**API Adaptation**

API requests can be transformed and adapted at various levels, including transport protocols, message formats and interface styles. CloudControl supports bridging between any supported protocol, including HTTP(S); (S)FTP(S); messaging products such as IBM MQSeries, Tibco EMS,
Layer 7 for vCloud APIs

ActiveMQ and various JMS implementations; SMTP/POP3/IMAP4; SSH and raw TCP sockets – Layer 7 also provides a transport SDK for adding new or custom transport mechanisms. At the message layer, content can be transformed to and from various formats such as XML, EDI, COBOL Copybook, and other flat-file formats. Of perhaps the most relevance to API exposure is the adaptation of interfaces between interface types – CloudControl provides simple but comprehensive mapping between SOAP, REST and JSON interfaces, including manipulation of HTTP methods, format mediation between XML and JSON, URL construction and parameterization, and construction of appropriate message constructs such as SOAP headers or SAML tokens.

API Message Routing
Messages can be routed to the appropriate API endpoints based upon a number of criteria including user identity, message content, time-of-day or availability. These criteria can be combined to create useful policies around multi-tenancy and elastic cloud expansion/contraction. For example, a user from a specific organization can be routed to an associated virtual datacenter based on geography, time of day, importance of the payload, and the health of that customer’s various endpoints. Routing operations include automatic failover from inactive endpoints to healthy instances of the same services or APIs.

API Composition & Orchestration
Orchestration of multiple APIs and composition of value-added interfaces that combine multiple backend APIs is accomplished using the transformation and routing capabilities discussed previously, along with a comprehensive set of workflow operations for flexible policy coordination. Iterative, conditional, looping and logical constructs allow for external callouts, fan-in/fan-out scenarios, and synchronous or asynchronous execution of logic. A series of internal API calls can be initiated with a single frontend request, allowing exposure of unique mash-ups and business processes. These calls can include any of CloudControl’s supported protocols, which enables control over multiple systems – for example, a self-provisioning call to a vCloud API can not only invoke the deployment of new virtual hosts and vApp instances, but also make SSH calls to manage new hardware and instantiate an associated storage solution.

API Credential & Data Caching
Custom caching configurations allow optimal performance for calls to the vCloud APIs without worrying about the latency introduced by a cloud-based solution. Identity attributes retrieved from an IAM system or XML configuration documents used to determine endpoint availability or routing preference can be cached and available for future calls – even full responses from a composite application API can be saved and re-used for a user-configurable time period. This caching mechanism can add state to a previously stateless interface, allowing for interactive API calls that remember user preferences and optimize for previous behavioral patterns.
API Metering & SLA

Metering and SLA enforcement on API requests allows a vCloud administrator to plan capacity according to expected request rates and take special action when traffic volumes increase beyond certain thresholds. CloudControl can enforce global throughput rates to prevent network saturation, or enforce user-specific SLAs for particular APIs, services, or endpoints. Traffic can be throttled or shaped when thresholds are exceeded, providing a respite for backend systems with limited resources – measured performance indicators include overall volume, latencies, message sizes, etc.

An API Gateway’s Operational Benefits to vCloud APIs

Layer 7’s CloudSpan CloudControl API Gateway manages and monitors APIs from initial implementation to production, through various development lifecycles and across multiple datacenters. It provides the visibility necessary to ensure service availability, while also providing business-level metrics for future prioritization. Operational capabilities providing value for exposed APIs include:

- Versioning of services/APIs/policies without having to modify application code
- High availability and clustering across multiple datacenters and network segments
- API lifecycle management between environments
- Real-time operational monitoring for endpoint health
- End-to-end service execution visibility
- Historical data collection for reports and metrics on service usage
- Integrated compliance auditing with custom parameters for targeted logs

API Versioning

API versioning is easily accomplished in CloudControl through the mediation of one service interface to another. For example, when upgrading from VMware vCloud API v1.0 to v1.5, CloudControl can expose a deprecated interface that’s mapped appropriately – v1.0 object IDs based on simple integers can be converted to unique-ID-based v1.5 object names, and v1.5-style version tags can be injected into the appropriate Accept header. This relieves the burden of supporting multiple interfaces within the application itself. Policy updates are pushed to gateways with no downtime necessary – new connections are simply processed by the new policies as in-flight transactions are completed. CloudControl policies are themselves automatically versioned, and historical policies are available for rollback at any point to avoid complications from regressions.

API Availability Assurance

For service providers exposing vCloud APIs for primary provisioning there is an expectations that the vCloud APIs are always available. The Layer 7 Gateways can balance API loads across multiple vCloud API instances even when geographically distributed. Using the clustering inherent in CloudControl gateways, peak loads can be accommodated across gateway clusters and load-balanced across endpoints. All CloudControl gateways support a clustering mechanism to provide fault tolerance, scalability, and simplified management. Cluster members automatically synchronize critical operating information such as policy and some counters so that they remain consistent and the
cluster has no single point of failure. The CloudControl administration console operates across the cluster as a whole. Clusters are managed across datacenters, geographical locations, and hardware or virtual form factor.

**API Lifecycle Management**

Layer 7 provides lifecycle management tools and infrastructure to move policies between distinct clusters or development environments. A command-line policy migration tool can copy the entire policy set from one cluster to another, automatically mapping location dependencies (such as hardcoded IP addresses) between environments. This application can be integrated with an existing build and deploy solution, and is most commonly used to migrate between development, test, and production environments. Alternatively, the Enterprise Service Manager (ESM) is a graphical interface that provides a GUI to drag-and-drop individual policies between cluster instances and surfaces environmental dependencies for a user-friendly mapping exercise.

**API Usage Monitoring & Reporting**

The CloudControl Management Console provides visibility into all APIs/services under CloudControl management. This includes information about rates of access, routing and policy failures. CloudControl instances keep data on an API-by-API and cluster member-by-member basis for several months; this usage data can be archived remotely for additional storage. Operational metrics can be viewed from the management console or distributed to existing operations infrastructure via standards such as SNMP, SMTP and syslog. A standards-based WSDM interface for external integration exposes information about current API rates of access, using both synchronous and callback models.

**End-to-End API Execution Tracing**

API calls can be tracked upon receiving messages, through any transformation, mediation or policy enforcement performed by the CloudControl gateway, and to their destination endpoints. Responses are similarly tracked, providing an end-to-end view of service execution and integrated system health. Service latencies and response codes from backend calls are available for real-time view or exporting for audit purposes.

**Historical API Usage Reporting**

CloudControl provides business-level users the historical usage information that they require to make decisions about future development investment. These reports can be generated based on user, API, or custom metric defined by an administrator – they can be viewed within the Enterprise Service Manager operational dashboard or exported and archived for future needs. Historical trends regarding vCloud API usage can give administrators a better understanding of how self-provisioning interfaces are being used by consumers of the API.
API Logging & Audit Compliance
CloudControl offers extensive logging and audit capabilities that can be tuned to meet specific customer compliance requirements. This includes general auditing of API access, but can include custom audit messages in response to events, or even persistence of entire message content. Audit and log data for transactions can be kept onboard in the virtual CloudControl image, integrated with syslog, or targeted to a specific audit destination. This audit capability augments the existing vCloud API logging and can contribute significantly to achieving compliance requirements in highly secure installations.

How an API Gateway Enables a vCloud Architecture

Introduction
The VMware vCloud Architecture ToolKit provides a set of guidelines for successfully deploying and validating virtual environments using VMware technologies, and is specifically targeted at the service provider market. It provides operational and organization suggestions and clearly delineates where functionality provided by VMware needs to be supplemented by additional technology to create a complete solution. The Layer 7 CloudControl API Gateway can meet many of these requirements to assist in the creation of a secure, robust cloud infrastructure.

Specifically, CloudControl addresses the following requirements from the vCAT best practices documents that dictate how to define, architect and operate a VMware vCloud:

- API Proxy to assist with vCloud API use cases
- vCloud cell load balancing
- Integration with the vCloud ecosystem
- Security and compliance of cloud deployments
- Workflow orchestration of multiple vCloud APIs
- Encryption and access control for API workflows

CloudControl as API Proxy for vCloud APIs
The VMware vCloud Architecture Toolkit – Architecting a VMware vCloud manual states that “it is important that a vCloud environment expose the vCloud API to vCloud consumers.” However, the shipped vCloud API provides only a basic security model (supporting only username/password authentication and support for SSL, with no advanced threat protection). Furthermore, the vCloud API is only hosted by vCD cells, which may not be readily accessible to external networks because the cells are behind a portal or simply not directly addressable from outside the management cluster. In this case, VMware recommends that an external proxy such as Layer 7’s CloudControl be deployed:

*To assist with the vCloud API use cases, the vCloud provider may want to implement an API proxy. The vCloud API is a REST-based service that contains XML payloads. For this reason, any suitable

---

XML gateway can be used to proxy the vCloud API. Several third-party solutions on the market today excel in XML gateway services. VMware collaborates with some of these vendors to develop joint guidance on how to deploy their solutions in a vCloud Director environment. For the latest information on these efforts and collateral, contact your local VMware vCloud specialist.2

CloudControl, acting as a policy enforcement point between vCloud API consumers and actual API endpoints, provides all of the necessary functionality for securing, managing, monitoring and orchestrating these vCloud API calls. In addition, CloudControl gateways can be deployed in the management cluster to protect any API – that includes Virtual Cloud Director, vSphere, vCenter Orchestrator, or any other application that hosts either a SOAP or XML service, or a RESTful API.

The following diagram illustrates protection of the vCloud RESTful API. The vApp administrators administer the CloudControl policies governing security, visibility, and management of these APIs. In this pattern, CloudControl is deployed in the distinct vCloud Management Cluster as a policy enforcement point in front of the vSphere server(s) hosting the vCloud API.

---

Figure 1: CloudControl integrated as a management component in the management cluster.

---

2 Ibid. Page 56.
If we take a closer look, we see that CloudControl is deployed in-line, so that all API traffic must flow through for policy enforcement. CloudControl assumes a deny-all security stance until administrators explicitly define policy for services under its management. Policy for access control, composition, or transformation of the vCloud APIs is then defined in a user-friendly graphical GUI and deployed to the CloudControl gateway.

Figure 2: CloudControl protecting the vCloud RESTful API.

**Load balancing vCloud Cells with CloudControl**

CloudControl virtual appliances cluster together (this is a CloudControl-specific cluster and should not be confused with the vSphere usage of “cluster”) to provide fault tolerance, scalability, and a single virtual point of management. The CloudControl cluster should reside between the vCD cells and the load balancer used to distribute load across the vCloud cells. Cell load balancing is described in section 3.6 of the VMware vCloud Architecture Toolkit – Architecting a VMware vCloud manual. The resulting architecture is depicted below:
Figure 3: CloudControl cluster protecting vCD cells hosting the vCloud API. The CloudControl cluster manages API access between an external network and one or more vCD cells.

Integration with the vCloud vApp Ecosystem
Layer 7 Technologies’ CloudControl API Gateway is a VMware Ready certified product that is deployed as a virtual image. It can be incorporated into the customer vApp catalog in the Infrastructure Apps section to support simple integration into customer vApps.

Security and Regulatory Compliance Using CloudControl
The VMware vCloud Service Definition document states:

Security and compliance continues to be one of the biggest barriers to adoption of the public cloud by enterprise customers. Most regulations and mandates in the industry, including SOX, PCI, HIPAA, COBIT, and ISO, have two areas of requirements: transparency/visibility and control.\(^3\)

CloudControl has undergone extensive compliance testing, including the following:

All cryptographic algorithms are certified to be compliant with FIPS 140-2 certification.

There are CloudControl instances available that have been awarded Common Criteria EAL 4+ status. This is consistent with the vSphere level of Common Criteria compliance testing that is currently underway.

CloudControl instances have undergone vulnerability testing for DoD STIG usage.

CloudControl has been engineered for inclusion in PCI-compliant architecture, and a PCI-DSS Secure Implementation Guide is available.

API Orchestration Using CloudControl’s Native vCloud Policy Assertions

CloudControl includes the ability to manage common vCloud operations, such as starting or stopping a vApp instance, within its palette of assertions that are used in policy definition. This makes the vCloud API a first-class citizen in the CloudControl Policy language, along with such fundamental operations as authentication, authorization, audit, message transformation, etc. The CloudControl policy language is similar to a graphical scripting language. It includes runtime variable evaluation, flow control, branching, logical comparisons, looping, termination, etc. Sophisticated workflows can easily be defined by using the vCloud API assertions in conjunction with the other CloudControl assertions.

Figure 4: vCloud API assertions in a CloudControl policy.

CloudControl for API Encryption & Access Control

It is important to recognize that these workflows are bound to the security policy, so they have the benefit of operating within an authenticated user context. This is consistent with the best practices advocated in the Operating a VMware vCloud guide:

> Because the orchestration workflows have access rights to multiple systems, the orchestration workflow code needs to be protected. Encryption controls such as Set Digital Rights management...
need to be enabled while moving workflow code packages within servers. Also, access to the orchestration servers must be limited.4

One example of how secure orchestration might be used is in a public cloud where the provider wants to extend the vCloud API to include a call to their proprietary billing engine every time one of their customers deploys a new vApp instance using the vCloud API interface. A CloudControl policy could be defined that creates a secure work flow to call the vCloud API to spin up a new application instance in the customer’s virtual network, and then also make a SOAP call to the provider’s billing engine. This is all done under the authenticated context of the cloud provider’s customer, thus it is ensured that there is a reasonable audit trail for all billable operations.

**Conclusion**

Exposing vCloud APIs enables valuable automation and management of application infrastructure in a public, private or hybrid cloud. However, exposing such direct control over the platform upon which applications are built also raises security, management and operational considerations. These concerns are detailed in VMware’s vCloud Architecture ToolKit and can be alleviated through the use of an API Gateway. Layer 7’s CloudControl API Gateway is suitable for any service provider or enterprise considering deployment of a VMware vCloud. CloudControl is available as a compact, high-performance virtual appliance that promotes widespread deployment through a vCloud ecosystem and simple integration with virtual apps. It is the only VMware Ready certified appliance for API management, and it provides the enterprise-level security and governance required for your vCloud deployment.

---

About Layer 7 Technologies
Layer 7 Technologies helps enterprises secure and govern interactions between their organizations and the services they use in the cloud; across the internet; and out to mobile devices. Through its award-winning line of SOA Gateways, Cloud Brokers and API Proxies, Layer 7 gives enterprises the ability to control identity, data security, SLA and visibility requirements for sharing application data and functionality across organizational boundaries. With more than 150 customers spanning six continents, Layer 7 supports the most demanding commercial and government organizations. Layer 7 solutions are FIPS-compliant, STIG vulnerability tested and have met Common Criteria EAL4+ security assurance. For more information, please visit www.layer7tech.com, email us at info@layer7tech.com or follow us on Twitter at @layer7.

Contact Layer 7 Technologies
Layer 7 Technologies welcomes your questions, comments, and general feedback.

Email: info@layer7.com

Web Site: www.layer7.com

Phone: 604-681-9377
1-800-681-9377 (toll free within North America)
+1 604 681 9377

Legal Information
Copyright © 2011 by Layer 7 Technologies Inc. (www.layer7.com). Contents confidential. All rights reserved. CloudSpan™ is a registered trademark of Layer 7 Technologies Inc. All other mentioned trade names and/or trademarks are the property of their respective owners.