Cloud Infrastructure Management Interface

CMWG Work Group

.

CMWG Current Work

A new computing paradigm is quickly emerging called Cloud Computing. Vendors and service providers have embraced the need to provide interoperability between enterprise computing and cloud service providers.

Virtualization technology and the evolution from software packages that can be created and deployed as a collection of virtual images is becoming the primary focus for delivering and managing software solutions into enterprise customers today. As these customers look to also take advantage of cloud computing, extensions are needed to enable interactions between private clouds within enterprises and between private and public cloud providers to exploit this emerging business model.

The Cloud Management WG will focus on addressing the management interfaces between the cloud service consumer / developer and the cloud service provider. The working group will also need to address the security mechanisms required to enable interoperability.

Virtualization & Cloud Management Forum

The goal of the VCM Forum is validation and interoperability of the virtualization, OVF, and cloud management standards.

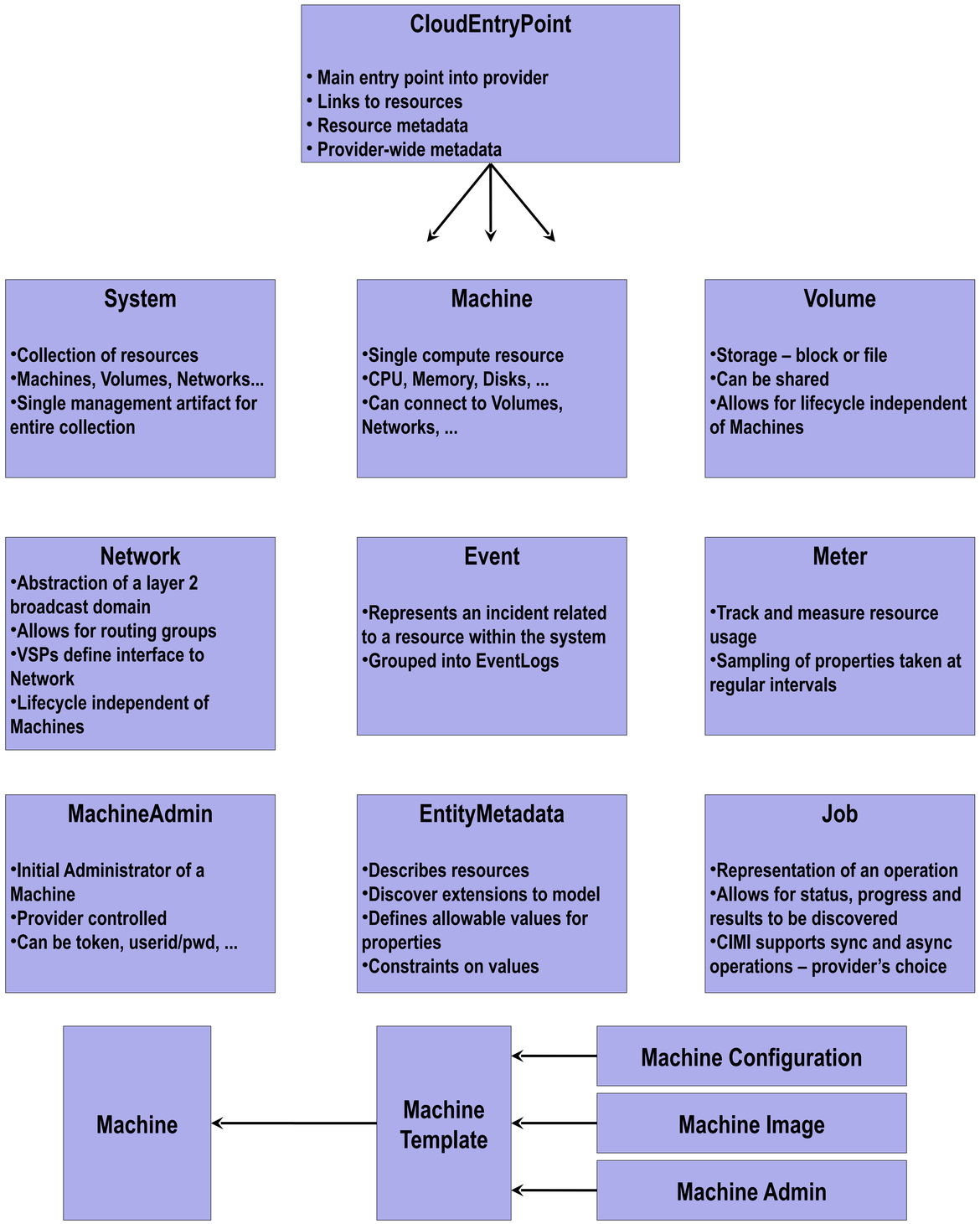
Relevant Websites

DMTF Published Standards
http://dmtf.org/standards/published_documents

DMTF Work in Progress Specifications
http://dmtf.org/standards/wip

Work In Progress Documents	
DSP#	Title
DSP0263	Cloud Infrastructure Management Interface (CIMI)
DSP0264	Cloud Infrastructure Management Interface – CIM (CIMI-CIM)
DSP2027	CIMI Primer

Cloud Infrastructure Management Interface Model



Cloud Infrastructure Management Interface Protocol

- The CIMI specification currently describes a REST/HTTP binding to the model.
  - Other bindings are anticipated.
- This protocol binding follows REST principles and describes mapping of the HTTP protocol verbs to operations on the model.
- Each resource in the model has its own MIME content type used in the Create, Read, Update and Delete (CRUD) operations.
- Standard HTTP status codes are used to convey the results of the operations.
- Serialization formats for the message body include JSON and XML
- CIMI-CIM describes the model in CIM

CIMI HTTP/REST Protocol Security

- Cloud Providers SHALL support secure HTTP connections using TLS.
- Cloud Providers MAY support non-secure HTTP connections.
- TLS 1.0, which shall be implemented, is specified in [RFC2246], and the TLS 1.1 and TLS 1.2 should be implemented as specified in [RFC4346] and [RFC5246], respectively.
- All CIMI clients and servers shall support the TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA cipher suite
- The TLS_RSA_WITH_AES_128_CBC_SHA cipher suite shall be implemented
- The TLS_RSA_WITH_NULL_SHA cipher suite (hexadecimal value shall be supported by both CIMI clients and servers to implement authenticated, non-encrypted communications
- The TLS_RSA_WITH_AES_128_CBC_SHA256 cipher suite should be included with all recommended TLS 1.2 implementations to meet the transition to a security strength of 112 bits
- Implementers are free to include additional cipher suites, but must prefer the mandatory ones in negotiation

Contact information

DMTF
Distributed Management Task Force, Inc.
www.dmtf.org

CMWG Work Group
cmwg@dmtf.org
cmwg-chair@dmtf.org

Workgroup Chair
Workgroup Chair: Winston Bumpus, VMware Inc.
wbumpus@vmware.com
Workgroup Chair: Mark Johnson, IBM
mwj@us.ibm.com