

Table of Contents

Part I: Securing Clouds 5

 The Open Question: July 2009 5

 Overview..... 5

 Background and Context..... 5

 Salient Use Cases 5

 SOAP/REST Web Services Mediation Obscured payloads Intracloud to public cloud service provider..... 5

 Federated Cloud Service Mashups (service to service single signon)..... 5

 Content Based Routing of Requests to Provider with the Data Set - in country data regulatory compliance..... 6

 Cost Trends are Down and Cloud == SOA + *aaS + HPCDG..... 6

 Current Business Pain: High Cost Structure..... 7

 Cloud is Strategy, Technology AND Business..... 8

 Application Development Process Infrastructure 8

 What is Needed? IT Operational Sourcing Options 9

 Zones of Privacy and Trust 9

 Virtual Data Store 9

 Process Management 9

 Development Capabilities..... 9

 Operational Risk Management 9

 What is being Protected? End to End Business Architecture 10

 Cloud Computing Security Challenges..... 12

 Data Privacy Regulations..... 12

 Healthcare: HIPAA..... 12

 Data at Rest..... 12

 Data in Motion 12

 Financial Services: GLBA and PCI 12

 Data at Rest..... 12

 Data in Motion 12

 Sovereign Jurisdiction: In-Country Data Location Requirements 13

 US, Canada, South America, EU Data Protection 13

 Dimension to Challenges 13

 Conceptual Challenges to Securing the Enterprise..... 13

 Definitional Challenges to Just Right Formal Requirements 14

 Operational Challenges to Service Quality Levels 14

Solutions 15

 The Distributed Edge of Private Clouds 15

 Cloud Capabilities..... 15

 Software as a Service 15

 Platform as a Service 15

 Infrastructure as a Service..... 15

 Environment as a Service..... 15

 Dynamic Trust Domains 16

- Loose coupling of policies to resources..... 16
- Late binding to SOAP/REST Web Services APIs 16
- Code and Data Integrity Protection..... 17
 - Payload Mediation/Transformation 17
 - Signature Validation on Envelopes, Software Libraries, and Component Classes .. 17
- Securing Common Cloud Use Cases 18
 - Use Case 1: SOAP/REST Web Services Mediation - Obscured payloads Intracloud to public cloud service provider..... 19
 - Use Case 2: Federated Cloud Service Mashups (service to service single signon) .. 20
 - Use Case 3: Content Based Routing of Requests to Provider with the Data Set -in country data regulatory compliance..... 21
- High performance Computing using Asynchronous Web Services (SOAP)..... 22
 - R&D 22
 - Monte Carlo Simulation Engines 22
 - Business Intelligence Analytics 22
- Data as a Service using Synchronous Web Services (REST)..... 23
 - Content Data Based Routing to Compute/Data Grid..... 23
 - In-country data regulatory compliance 23
 - Low latency execution 23
- Part II: An Open Architecture—An Open Narrative 24
 - Guiding Principles 24
 - First Five Principles from the CSA 1.0 Guide..... 24
 1. Abstraction of Infrastructure..... 24
 2. Resource Democratization 24
 3. Services Oriented Architecture 24
 4. Elasticity/Dynamism of Resources 24
 5. Utility model of Consumption & Allocation 24
 - Second Seven Extensions 25
 6. Work is distributed. Control is centralized 25
 7. No unauthenticated or unauthorized traffic behind the enterprise firewall. . 25
 8. Security policies are transparent to applications..... 25
 9. Resources are DOS attack resistant. 25
 10. All interactions are policy filtered, exceptions being logged, as well as, acceptances. 25
 11. Security policies, services and tools inter-operate among internal and external systems..... 25
 12. Architecture scales up and down with users, data, interactions and/or transactions. 25
 - Operating in Clouds 26
 - Cloud Deployment Models 26
 - Private Clouds 26
 - Community Clouds 26
 - Public Clouds 26
 - Hybrid Clouds..... 26
 - Cloud Ecosystem Stack..... 26

- Operational Cycle of Clouds—it’s all about the virtuous cycle of abstraction 27
- Standard Cloud Security Functional and Capability Categories..... 28
 - Authentication..... 28
 - Authorization 28
 - Audit/Non-Repudiation..... 28
 - Data and Messaging Privacy..... 28
 - Data and Messaging Integrity 28
 - Operational Monitoring 29
- XACML Architecture: A very short tutorial 30
 - Overview..... 30
 - Components of the Architecture 32
 - PEP: Policy Enforcement Point 33
 - PDP: Policy Decision Point 33
 - PIP: Policy Information Point 33
 - PAP Policy Enforcement Point..... 33
 - Policy Suite as Definition of a Unit of Security Work 34
 - Characteristics of the components of the Architecture 34
 - PEPs are Local 34
 - PDPs are Federated 34
 - PIPs are Distributed 34
 - PAPs are Centralized 35
- Policy Development Process and Supporting Components..... 36
 - Components Supporting Policy Development and Operations 36
 - A Duty Dozen: BP2Ops 36
 1. Business Process 37
 2. Work Flow Design Patterns 37
 3. Use Case Policy Templates..... 37
 4. Policy User Interface..... 38
 5. Policy Information Point..... 38
 6. Policy Administration Point..... 38
 7. Policy Repository Service..... 38
 8. Policy Test Workspace 39
 9. Policy Decision Point..... 39
 10. Policy Enforcement Point 39
 11. Operational Component 39
 12. Policy Monitor Audit Log..... 39
- Policy State Life Cycle from Definition to Master Operational Copy 39
 - Policy Suite Life Cycle 40
 - Created 40
 - Meaningful 40
 - Consistent..... 40
 - Complete 40
 - Certified 40
 - Deployed 40
 - Deprecated 40

Reference Behavior..... 41
A Note on Determining Commodity and Premium Intellectual Property 41

Conclusions..... 42
Current State of the Art..... 42
Next Steps 42