Computación en la nube:
beneficios, críticas y aspectos de interés para la Informática Forense

Corrado Federici
corrado.federici@unibo.it

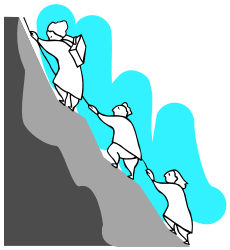
"En medio de la dificultad radica la oportunidad"
Albert Einstein

Ciclo de seminarios sobre perfiles jurídicos y tecnológicos de la Informática Forense
Tenerife 16 de mayo 2012

¿De qué hablaremos?

- Principios básicos de la Computación en la nube (CN)

- Ventajas e inconvenientes de la CN como modelo de negocio



- Desafíos y consideraciones para la Informática Forense en el contexto CN

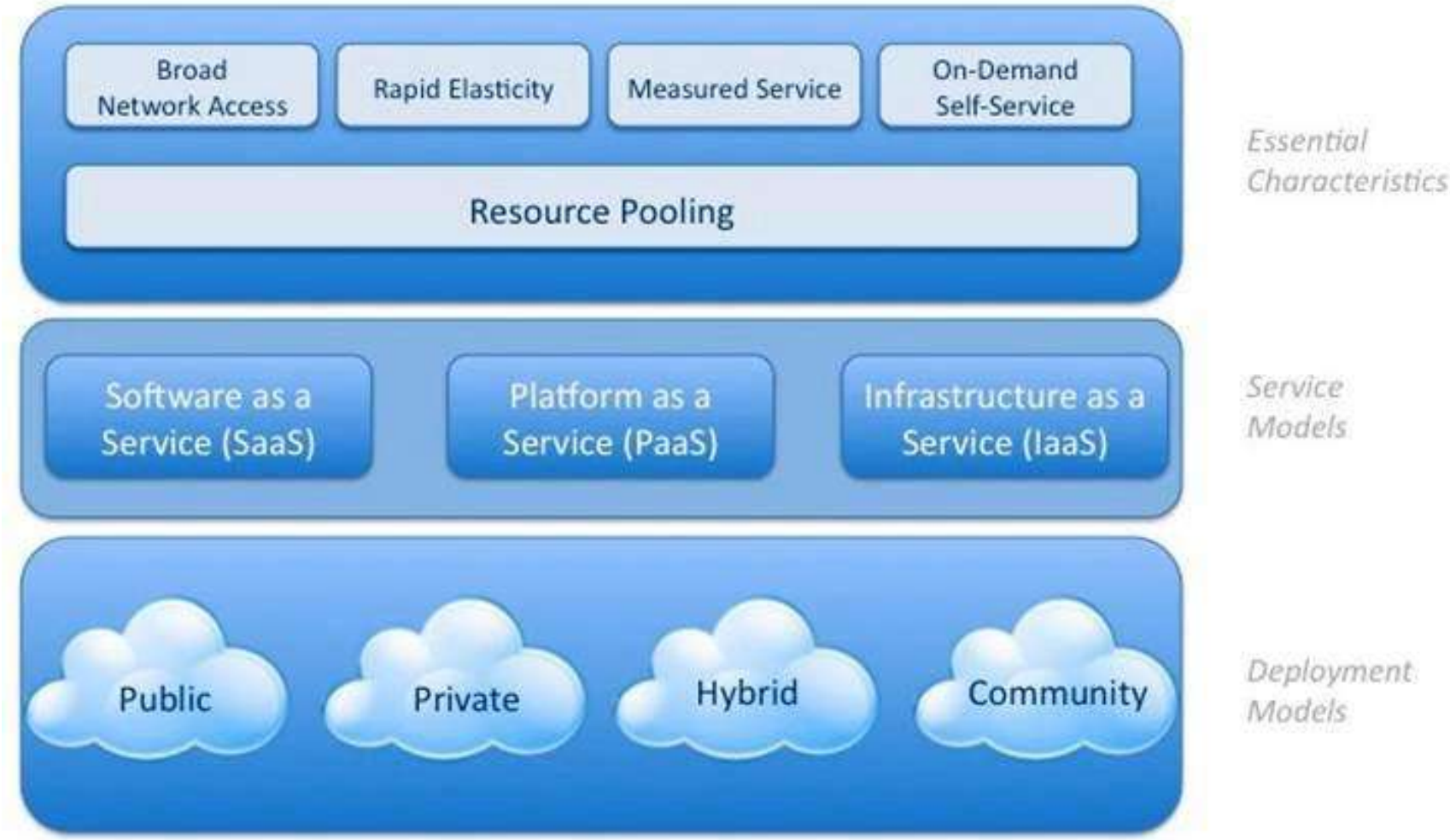
Computación en la nube

Principios básicos

¿Qué se entiende por Computación en la nube?

- Es el concepto de “ICT” como servicio
- Es el sueño del ordenador como “utility” hecho realidad: se paga por el consumo efectivo, como en el caso del agua, la electricidad o el gas
- Es la disponibilidad constante de servicios ICT a buen precio que son suministrados a través de una red, tarifados solo por el tiempo real de utilización
- Los puntos de referencia geográficos son mucho más delicados respecto al tradicional alojamiento

La definición formal de CN (NIST)



Modelos de servicio: SaaS

- El usuario final alquila una plataforma software preconfeccionada con aplicaciones para la productividad de oficinas, CRM, ventas, BI y otros

- SaaS permite a una organización concentrarse en el núcleo del negocio
- Desde el punto de vista técnico, ningún problema para la gestión de la infraestructura. Responsabilidad solo por aspectos concretos como la configuración imprudente o descuidada

- Sin embargo, no hay ningún control sobre los aspectos claves como el formato de los datos o las técnicas de protección

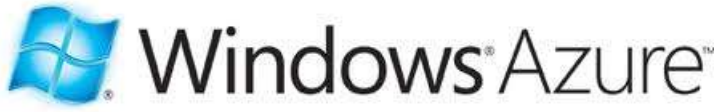
Modelos de servicio: PaaS

- Los usuarios pueden desarrollar aplicaciones desde cero con lenguajes de programación de alto nivel como Java o C# que aprovechan los recursos hardware del CSP
- Esto es posible gracias a una interfaz aplicativa (API) expuesta por el CSP (normalmente propietaria)
- El cliente es responsable por los defectos del software causados por errores en la escritura del código o por configuraciones descuidadas
- Aún ningún cargo resultante de la gestión del sistema informativo

Modelos de servicios: IaaS

- Es un centro de datos virtual a disposición del usuario, en el cual vienen garantizadas las credenciales de la administración de las máquinas virtuales
- Amplia libertad en la elección de los sistemas operativos, tecnologías de base y lenguajes de programación
- Comporta la gestión lógica del sistema informativo
- Responsabilidad compartida entre el cliente y el CSP que slo mantiene el control de la infraestructura subyacente (desde el Hypervisor hasta la seguridad física)

Los CSP más conocidos ¿Notan algo?



¿Algo viejo con nuevo nombre?

La CN está basado en tecnologías consolidadas:

- Continuidad del negocio
- Baja utilización media de los sistemas informáticos
- Picos de la demanda no gestionados
- Adquisición duradera de bienes y servicios

Lo cierto es que no. Los factores claves son:

- Los servicios IT a buen precio están disponibles gracias a un cambio de opinión radical en la gestión de los centros de datos
- Economías de escala en la adquisición de bienes y servicios
- Uso del hardware básico (**COTS: Commodity Off the Shelf**)
- Cultura DEVOPS que lleva a una elevada automatización, muchos versión/día del software y alta relación computador/administrador

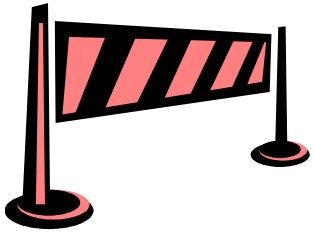
Lo cierto es que no. Los factores claves son:

- ✓ Menor disponibilidad económica para configurar las granjas de servidores tradicionalmente subutilizadas
- ✓ Las aplicaciones pueden exportarse de la red local al CN gracias a un aumento de la banda ancha
- ✓ Oferta de aplicaciones ya hechas que pueden ser modificadas a gusto del cliente

¿Qué ofrece la Computación en la nube?

Beneficios y críticas del CN como modelo de negocio

Beneficios



- **Salida fácil**: para quien comienza un negocio sin ninguna dedicación a largo plazo o costes iniciales

- **Plataforma IT elàstica**: los recursos computacionales y de almacenamiento pueden crecer para hacer frente a picos de demanda o disminuir en tiempos muertos. Un CSP ofrece una disponibilidad del 99.9 % o superior.

- **Ningún calvario de aprovisionamiento**: se compran servicios, no activos. Los gastos en capital (CAPEX) son conmutados en gastos de servicios (OPEX)

http://knol.google.com/k/-/-/q38vklbh61ib/mi4kay/coil-springs.jpg

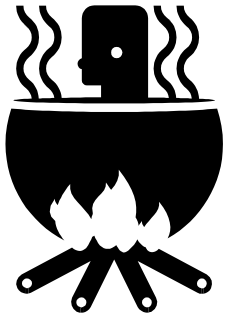
Oportunidades

- **Delegación de la gestión de las TI**: el trabajo necesario para mantener los datos íntegros, disponibles y reservados en cumplimiento de las normas se comparte con el CSP
- **2a juventud del SW**: **las** aplicaciones agotado pueden ser revisadas con instrumentos de desarrollo modernos que confieren más reactividad, atractivo y capacidad de resistir a los cargamentos de pico
- **Creación de valor**: mejores aplicaciones convierten las TI en aspecto estratégico, no solo por los ahorros que supone, sino también porque los nuevos productos contribuyen al negocio de la empresa

La CN es perfecta para:

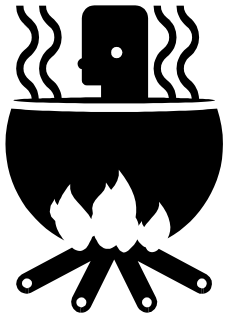
- ✓ Empresas jóvenes
- ✓ Para bancos de pruebas que podrían funcionar, pero también no
- ✓ Para necesidades que tienen una duración limitada (la B.I. en una campaña electoral)
- ✓ Para elaboraciones caracterizadas por picos de utilización (conocidos o desconocidos)

Críticas



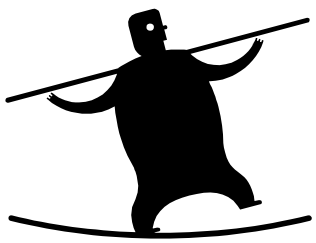
- **Pérdida de control**: la exportación de datos de valor fuera del perímetro empresarial comporta problemas acerca de la confidencialidad y disponibilidad de los datos
- **Respecto de las normas**: la computación no es todavía un sistema con normas compartidas a nivel internacional
- **Respecto del SLA**: verificar el cumplimiento por parte del CSP puede ser imposible (Ej. El wiping de los soportes según los estándares o el confinamiento de datos en una región). Esta oferta es todavía poco transparente

Aspectos que preocupan



- **Seguridad**: la falta de seguridad física o lógica (vulnerabilidad de un ambiente multi-usuario puede generar intrusiones desde el exterior o desde el interior
- **Concentración de valor**: como los bancos las plataformas de los CSP son objetivos atractivos para los cibercriminales
- **Bloqueo**: si el CSP usa un formato de datos propietarios, podría ser mucho más difícil y/o caro para los usuarios cambiar de proveedor

Un asunto de gestión del riesgo



- Trasladar los servicios TI hacia la CN no es tanto un problema técnico, sino más bien de **risk management** (e.g. NIST SP 800-37: A risk management framework for Federal Agencies)
- La gestión debe equilibrar beneficios y riesgos, incluyendo y reduciendo los segundos a un nivel aceptable, evitando perseguir expectativas poco realistas

La Computación en la nube según el supervisor

- La autoridad italiana de protección de la privacidad ha publicado una guía para el uso consciente de los servicios de CN
- Delegar a terceros la gestión de TI no exime a las empresas y a las AAPP de la responsabilidad derivada de las normas sobre la protección de los datos personales

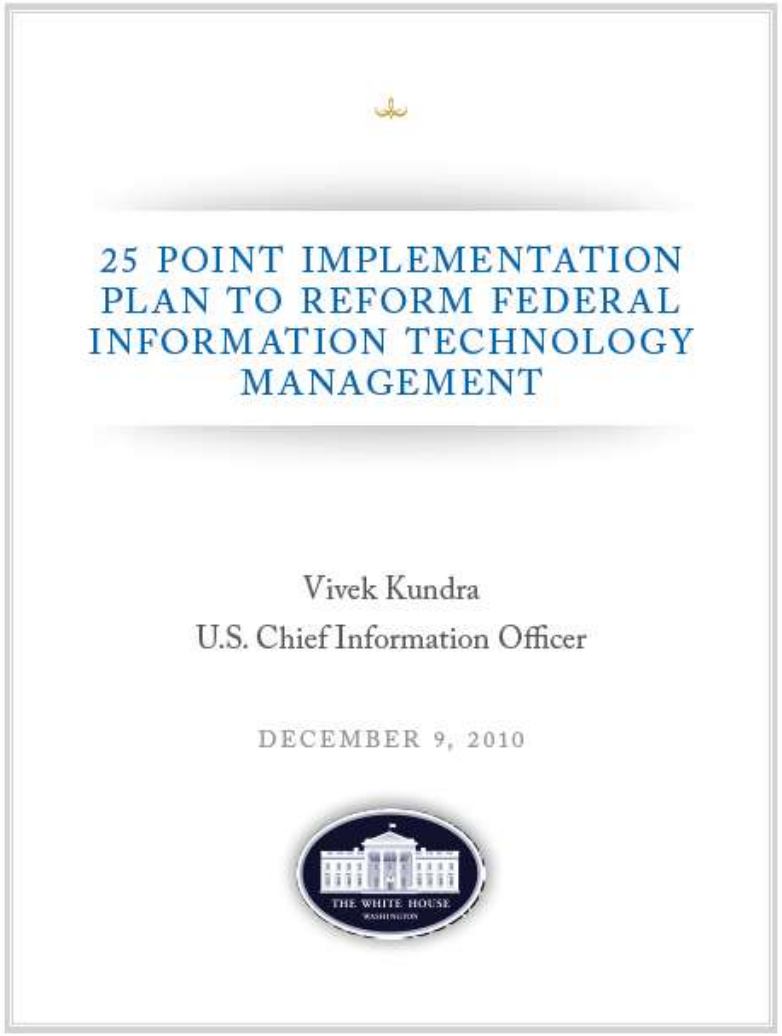
Computación en la nube y privacidad: decálogo

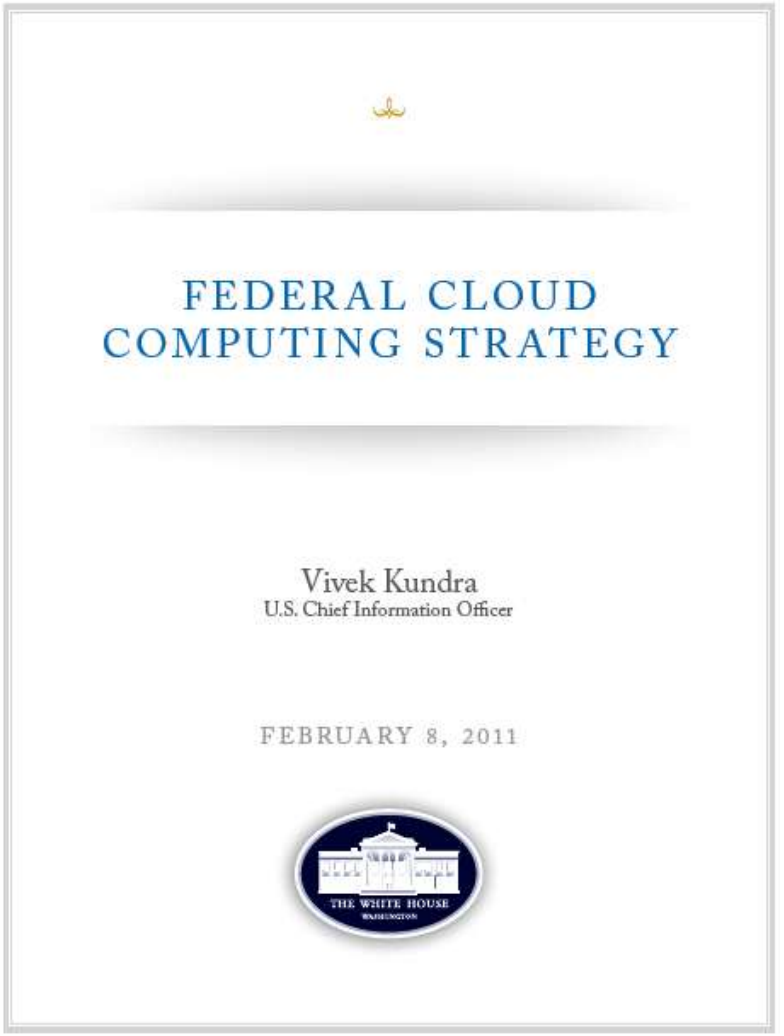
- Evaluar la relación riesgos-beneficios, sobre todo en relación con la naturaleza de los datos: ¿qué pasa si los datos vienen revelados, se borran o no están en línea?
- Verificar la fiabilidad del proveedor/es (referencias, políticas de seguridad y de continuidad en el negocio, certificaciones, posibilidad de negociar un SLA…)
- Privilegiar CSP que garantizan la portabilidad de los datos
- Asegurarse copias locales de los datos para los casos de emergencia
- Informarse sobre la localización real de los datos
- Cuidados en el SLA: las responsabilidades del CSP, protección de datos, políticas de recuperación

¿Y cuál es la estrategia europea?

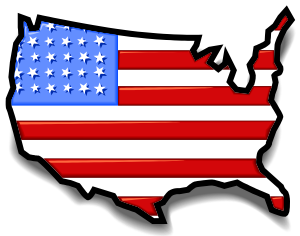
- Trabajos orientativos de la ENISA:
  - *Computación en la nube: Beneficios, riesgos y recomendaciones de seguridad (Nov,2009)*
  - *Security & Resilience in Governmental Clouds Making an informed decision (Enero, 2011)*
- DigitalAgenda (Mayo 2010)
- Anuncio público (27 de Enero 2011)
- Consulta pública (Mayo-Agosto 2011)
- Coloquios con CSP, PMI y usuarios profesionales
- Presentación del documento de estrategia previsto para el 13 de junio 2012 de la Computación en la nube en el World Forum de Londres

La CN en el exterior: el ejemplo de los Estados Unidos





Cloud First Policy

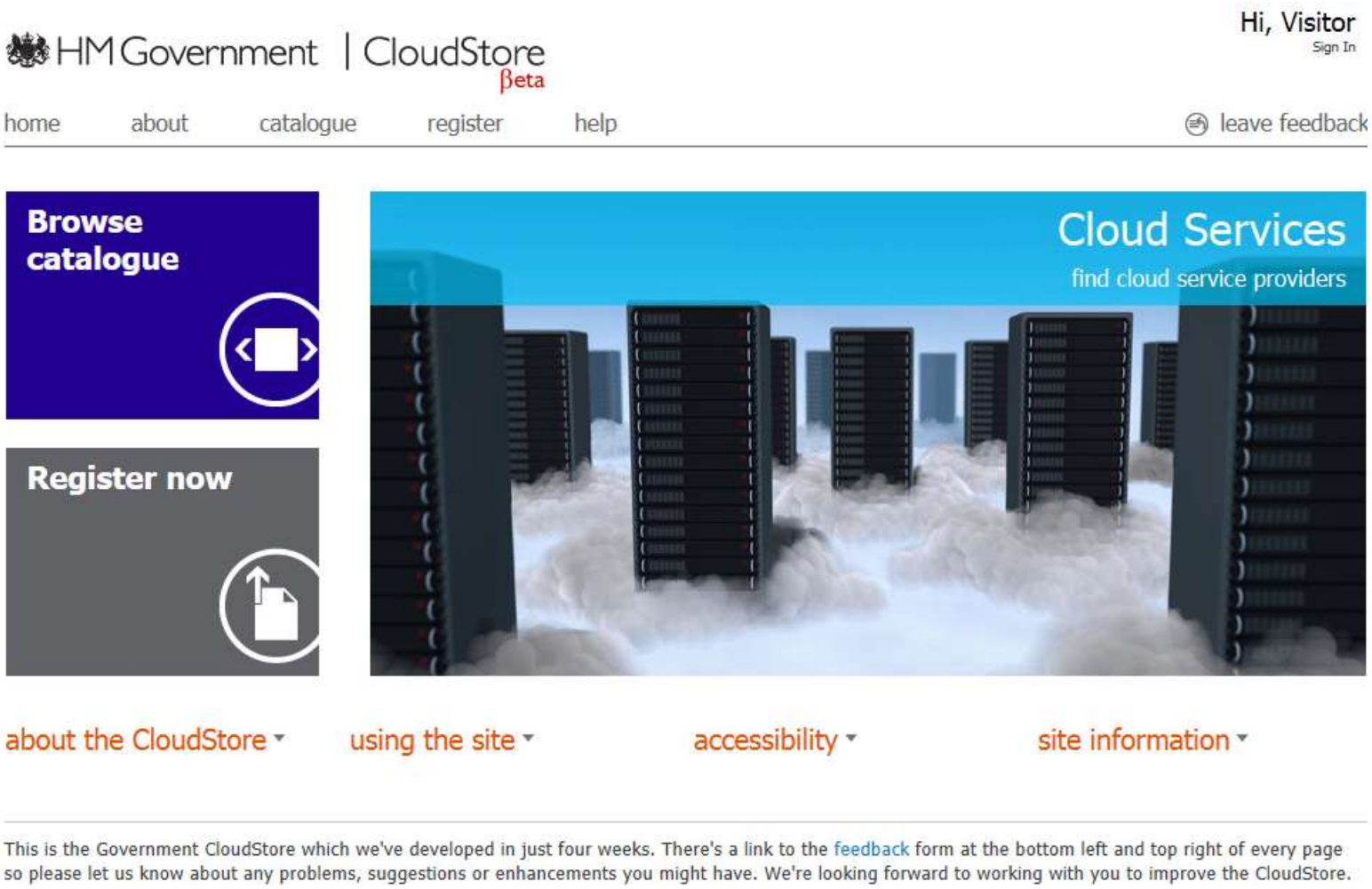


- Fue creada la Cloud First Policy que obliga a los CIO de todas las agencias federales a identificar, dentro de 3 meses, 3 proyectos con el fin de avanzar hacia la CN dentro de los 18 meses siguientes.
- Esto porque:
  - Muchos proyectos sobre TI superan el presupuesto y no alcanzan los beneficios previstos
  - Existe una galaxia de plataformas TI federales de las que no se habla, que tienen elevados costes de adquisición y mantenimiento y son utilizadas por un tiempo determinado
- La cuarta parte del presupuesto federal en materia de TI puede ser traspasado a la CN (¡¡¡20 millones de dólares!!!)

Apps.gov


GSA
Apps.Gov
A Service Provided by GSA
Welcome Register | Log In
0 Items in Cart $0.00
Contact Us | Cloud FAQs | Vendor FAQs
Home Business Apps Productivity Apps Cloud IT Services Social Media Apps Info.Apps.Gov
Tuesday, April 24, 2012
SEARCH FOR
IN All Categories
GO
Introducing new Cloud IT Services!
GSA is happy to introduce cloud storage, virtual machines and web hosting services to Apps.gov. Click on the Cloud IT Services link below to view contractors offering these services. We're just beginning, so stay tuned for expanded functionality and offerings under Cloud IT Services.
What is Cloud Computing?
Want to learn more?
Watch this brief video for an overview of Cloud Computing to gain a better understanding of what it is and its benefits.
Watch the video now »
Video transcript »
What type of solution do you need?
Business Apps
Your agency or service is complex and requires state-of-the-art software to get business done.
GSA Cloud Business Apps has a solution!
Cloud IT Services
Need a better solution to reduce cost and implement projects faster?
GSA Cloud IT Services has the answer!
Productivity Apps
You need to get things done and GSA is there to help you do just that.
GSA Cloud Productivity Apps has the tools!
Social Media Apps
Social media tools make it easier to discuss the things we care about and help us get the job done.
GSA Social Media Apps can help you get the word out!

UK Cloud Store el portal del G-Cloud



La Computación en la nube como un instrumento

¿La CN puede ayudar a la Informática Forense?

Computación en la nube y CF

- Gracias a la enorme variedad de tecnologías (también propietarias) usadas por los CSP, la Informática y la network Forense en la nube pueden representar un desafío para el experto forense
- Las mejores prácticas y procedimientos formales consolidados en el tiempo (ejemplo: NIST SP 800-86) que exigen la completa adquisición mediante bitstream copy, podrían no ser aplicables en el medio CN
- Sin embargo, la difusión de la CN puede ofrecer a la CF beneficios sin precedentes

Los problemas de la moderna CF

- Los dispositivos electrónicos son cada vez más heterogéneos, capaces y conexos
- Un caso forense medio requiere mucho espacio en el disco y una gran potencia del CPU para ser tratado en un tiempo razonable

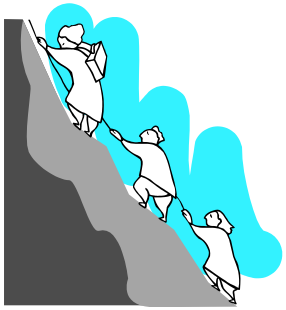
Los problemas de la moderna CF

- Demasiados casos para equipos de expertos infradimensionados: falta de tiempo
- Falta generalizada de recursos económicos: reducida capacidad para invertir en equipamiento técnico
- Necesidad de realizar un análisis global del patrimonio informativo de las investigaciones y no por cada concreto medio de prueba
- Voluntad de acceder por vía remota a los resultados con cualquier dispositivos fijo o móvil

Beneficios de la CN para la CF

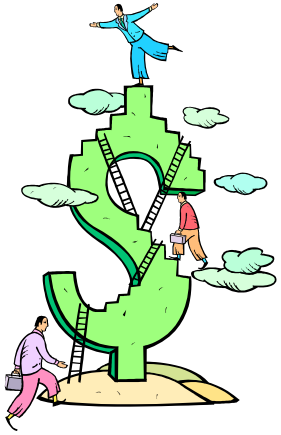
- La Informática Forense puede disfrutar de la enorme capacidad de procesamiento distribuida por la CN para almacenar y analizar los resultados
- Las herramientas forenses desarrolladas por la CN podrían avanzar de forma horizontal sin límites
- Los fragmentos de cada resultado (ejemplo: los ficheros) podrían ser asignados en paralelo a muchas unidades de elaboración y consolidadas en un resultado final (MapReduce)
- Las herramientas podrían estar basadas en tecnologías de código abierto que minimizarían el problema del bloqueo y aumentarían la transparencia

La Computación en la nube como blanco



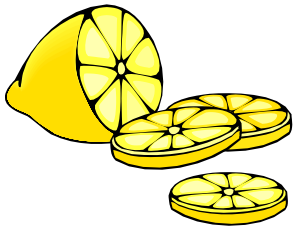
Desafíos para la Informática Forense: la CN como objeto de investigación

Desafíos para la CF: la nebulización de los datos



- Un acceso directo a los dispositivos mediante el secuestro o el aseguramiento vía bitstream podría ser una pesadilla para los locales del CSP, sin afectar a su negocio
- De hecho, las aplicaciones CN deben avanzar permaneciendo reactivas y tolerantes a los fallos o desastres
- Los servicios CN deberán además, costar poco y eso requiere el uso de COTS

Desafíos para la CF: la nebulización de los datos



- Todo esto es obtenido distribuyendo fragmentos de datos sobre diversos ordenadores, que en potencia podrían estar geográficamente distantes (ejemplo **Google FS** o **Cassandra** database)
- Reconstruir una fotografía unitaria en ese escenario, distribuida de manera impecable bajo el perfil forense podría ser una empresa desesperada

- Idear soluciones no rigurosas rebajaría el nivel de calidad de comprobación, con el consiguiente conflicto durante el debate

Desafíos para la CF : la subcontratación

- Muchos CSP son, a su vez, clientes de la CN dado que se confían a las plataformas de otros (ejemplo: Dropbox se apoya en Amazon S3)
- Esto podría obligar al investigador a dirigirse a CSP de diversos países, que usan tecnologías completamente distintas
- Piénsese, por ejemplo, en el caso de un proveedor belga que produce una aplicación para la productividad de la oficina, pero usa máquinas virtuales y espacios backup confiadas a sociedades francesas y alemanas

Desafíos para la CF : la permanencia de los datos

- La CN tiene Pros y Contras respecto a la permanencia de los datos
- Con un tipo de disponibilidad del 99.9 % o más, es probable que la CN "*no olvide nada*"
- Varias copias de los datos (**Versioning**) podrían estar disponibles en distintos lugares (potencialmente separados y bajo jurisdicciones separadas)
- La posibilidad de encontrar las copias útiles de datos depende mucho de la calidad del servicio suscrito por el target

Desafíos para la CF: la permanencia de los datos

- Por el contrario, la naturaleza de autoservicio de la CN podría convertir las valiosas informaciones en extremadamente volátiles
- Los recursos pueden ser asignados también por pocas horas de modo "*rectangular*" (ejemplo: 20 VM para una hora cuestan como 1 para 20 horas) y, por tanto, abandonado
- Los datos de la actividad criminal podrían ser sobrescritos rápidamente cuando las zonas de disco se vieran asignadas a otro cliente
- Este 'ir y venir' se ve posteriormente favorecido por políticas agresivas de marketing del CSP (ejemplo: Amazon EC2 spot instances)

Desafíos adicional

- Los beneficios de la CN de sacrificar la inversión inicial valen también para la delincuencia
- Como la mejor práctica, los usuarios podrían inclinarse a cifrar los datos antes de introducirlos en la CN pública (en relación con la CN privada)
- Los formatos de datos propiedad del CSP pueden implicar cambios mediante instrumentos no documentados, lo que podría plantear asperezas en el debate

Ejemplo : Amazon S3 object store

- Sirviéndose de Simple Storage Service, los clientes de Amazon pueden almacenar y recuperar los “objetos digitales” con independencia de la cantidad (foto, video, documentos ..) por cada sitio web
- Non es un File System. Para ser modificados, los objetos deben ser cancelados y reimportados en la plataforma
- Las políticas de redundancia hacen más copias en dispositivos distintos dentro de una región, obteniendo una disponilidad del 99,99%
- El mecanismo de Versioning protege de las cancelaciones involuntarias o por defectos de programación del software

Ejemplo: Amazon S3 object store

- Amazon S3 utiliza un mecanismo de registro (log) opcional del acceso a los objetos
- Este registro es desactivado para configuración predefinida
- Las aplicaciones que usa Amazon S3 mediante servicios web pueden también contar con un cifrado opcional **AES a 256 bit** (lato Server) o bien, almacenar objetos ya criptografiados (como se aconseja para la CN pública)
- **DropBox** (www.dropbox.com) usa este código
- **BoxCryptor** (http://www.boxcryptor.com/) es una aplicación para cifrar los datos de usuarios antes de guardarlos dentro del Virtual Box folder: se tienen, así, dos niveles de cifrado

Consideraciones

- Acceder directamente a los datos brutos es, de hecho, difícil dada la incapacidad técnica para identificar soportes digitales importantes en un datacenter, que puede estar situado en el extranjero

- Una investigación, por tanto, deberá contar con los datos extraídos del CSP por cuenta de una parte del proceso (copias de las VM, ficheros, log de acceso y de las operaciones)
- Para cumplir los principios generales de fiabilidad, pertinencia y exhaustividad de los resultados digitales, es fundamental la colaboración del CSP en relación con los procedimientos de adquisición

Consideraciones

- Los SLA genéricos son polarizados hacia el CSP y podrían incluir un pequeño conjunto de procedimientos en soporte de incidentes informáticos

- Registrar la información frena la ejecución de los procesos de las máquinas y cuesta en términos de espacio en el disco. Los log se ven obligados, probablemente, a un nivel mínimo si no se acuerda otra cosa
- Los indicios importantes podrían ser unos pocos y, por tanto, deben ser extraídos de acuerdo con las mejores prácticas

Consideraciones

- La actividad práctica de extracción de datos será realizada por administradores de sistemas que podrían utilizar instrumentos de poco valor desde el punto de vista forense (quizás aún por crear para la tecnología CN utilizada), pero solo script para el mantenimiento normal
- Si es posible, una interacción preventiva de un técnico forense para compartir procedimientos e instrumentos, puede evitar comprometer una investigación

Consideraciones

- Considerada la extrema variabilidad de los procedimientos en función de las tecnologías adoptadas por el ISP, debería alcanzarse un acuerdo sobre la estrategia de los datos y su nivel de integridad
- El conocimiento de las principales plataformas CN (**Openstack, CloudStack, VSphere**..) podría ser de gran importancia

Consideraciones

Todo esto en espera del momento en que los CSP estén dispuestos a producir también:

Forensics as a service

Según condiciones de suministro lo más documentadas posible y certificadas en función de las mejores prácticas forenses

Notas finales: la formación

- Hacer investigaciones en CN requiere un aumento de la conciencia de los técnicos forenses en las siguientes áreas:
  - Software para la gestión de plataformas CN y web services
  - File systems paralelos y database distribuidos
  - Lenguajes de programación y técnicas de scripting
  - Redes
- Esto para no fiarse de forma pasiva de los datos suministrados por el provider, que podría haberlos obtenido sin los procedimientos y garantías necesarias

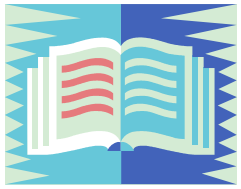
Notas finales: cooperación

- La naturaleza potencialmente dispersa y efímera de los datos de la nube requiere una colaboración 247/7/365, que se hace aún más apremiante entre las naciones, dado que la variable tiempo en una investigación de éxito se ha convertido en un aspecto todavía más importante
- Los procedimientos técnicos compartidos aplicados al ambiente CN, contribuirían a garantizar una correcta identificación y adquisición de los resultados; sobre todo en actividades conjuntas entre países distintos

Notas finales: la conciencia

- Muchos países no tienen todavía una estrategia formal a nivel nacional
- No debe extrañarnos que los retos de la Informática Forense en el ambiente CN parezcan ser, en caso de que sean considerados, subestimados
- En consecuencia, los tradicionales instrumentos técnicos utilizados podrían resultar completamente inadecuados en un escenario de la Computación en la nube

Bibliografía



- **Federici**,**C** & **Mauro,A.** *Cloud Computing for Government and Military* in Security and Privacy in organizational Cloud Computing, IGI Global 2011 (to be published in 2012)
- **Reilly & Al**. *Cloud Computing: Forensic Challenges for Law E*Conference, 2010*nforcement* in Internet Technology and Secured Transactions
- **Taylor,M & Al**. *Forensic Investigation of Cloud Comput*ting *Systems***,** Elsevier 2011
- **Taylor,M & Al.** Digital evidence in Cloud Computing Systems**,** Elsevier 2010
- **Barret,D & Kipper,G***: Cloud Computing and the forensic challenges* in Virtualization and Forensics, Syngress 2010
- **Garfinkel,S.L**. Digital forensic research: the next ten years, DFRWS 2010
- **Bias, R.** *Elasticity is NOT #Cloud Computing … Just Ask Google.* Cloudscaling.com 2011

Gracias por vuestro tiempo

Corrado Federici
PhD Candidate in Computer Forensics
University of Bologna , CISFID
corrado.federici@unibo.it
skype id: blueye.it