Windows Azure

Security Considerations

Matthias Luft

mluft@ernw.de

Who we are

- Old-school network geeks, working as security researchers for
- Germany based ERNW GmbH
  - Independent
  - Deep technical knowledge
  - Structured (assessment) approach
  - Business reasonable recommendations
  - We understand corporate
- Blog: *www.insinuator.net*
- Conference: *www.troopers.de*

Agenda

- Introduction & Definitions
- Azure Infrastructure
- Threat Models & Security Implications
- Conclusions

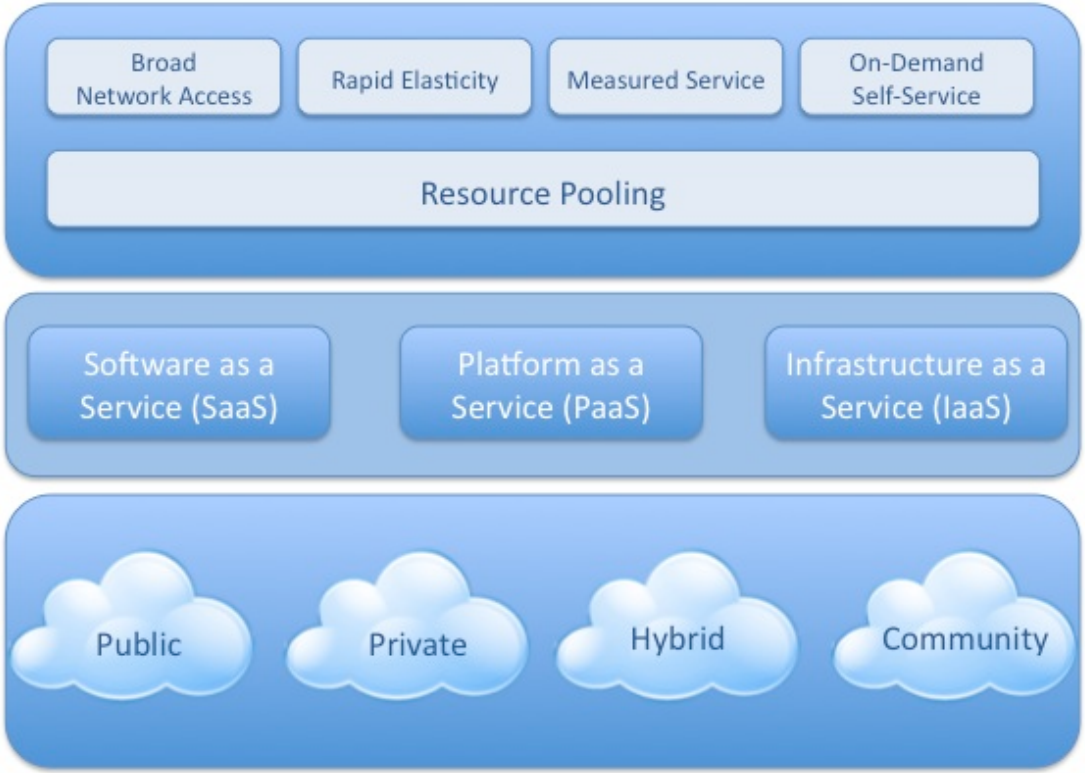
What is *the Cloud*?

Buzzwording

- "Think stateless CPU in the Cloud"
- "The unique architecture of the cloud not only offers unlimited storage capacity, but also lays the groundwork for eliminating the daily grind of data backup thanks to the cloud's constant replication of data."

Security Concerns

- “Where is my data stored?”
- “Who has access?”
- “Do I have to take care of backups?”
- “Is the service secure?”
- “Can I be compliant in the cloud?”



Essential Characteristics

Service Models

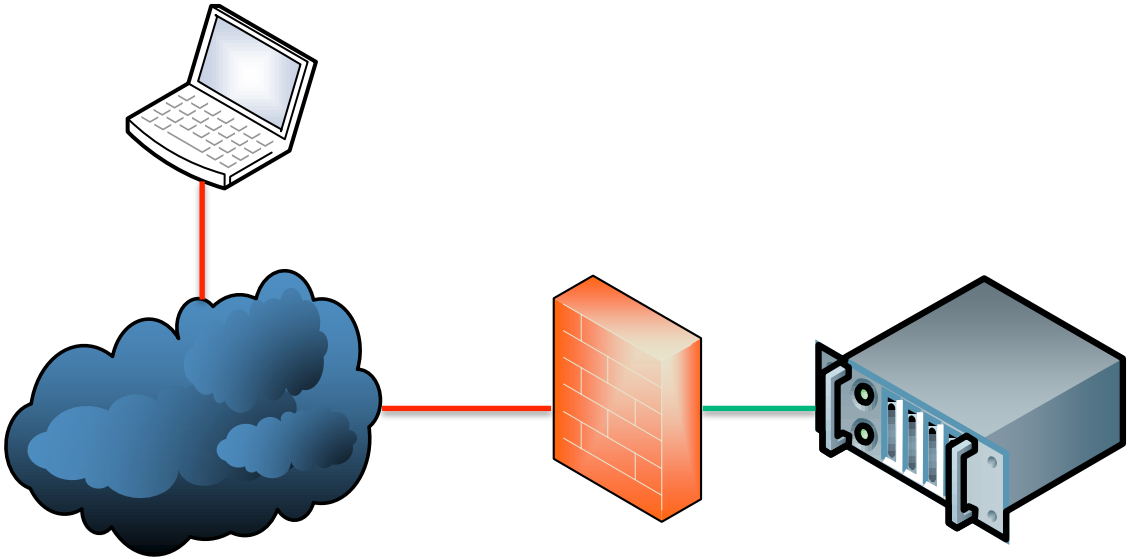
Deployment Models

Definition of Cloud Computing

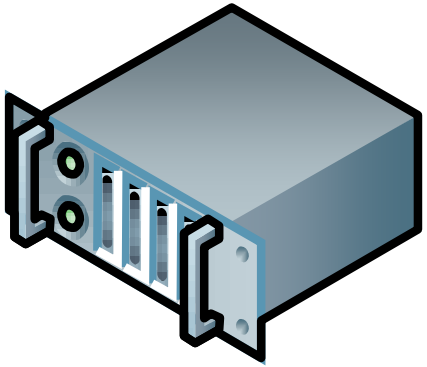
Well said...

- ... but how does this help?
- Let's put on the "infrastructure/ security glasses".
  - Getting an understanding of actual cloud infrastructure.
  - Derive changes in threat models.
  - Recognize new security challenges.

The (really) old World

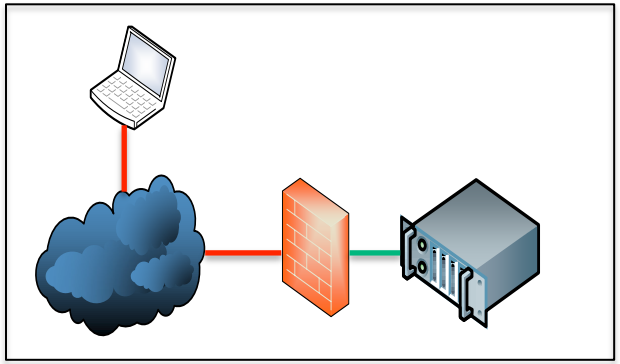


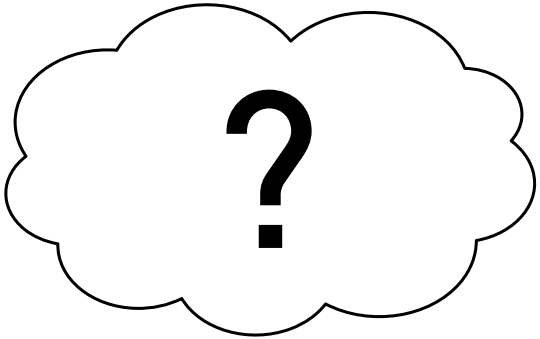
The new Virtualized World



Virtual Workload

The new Cloud World

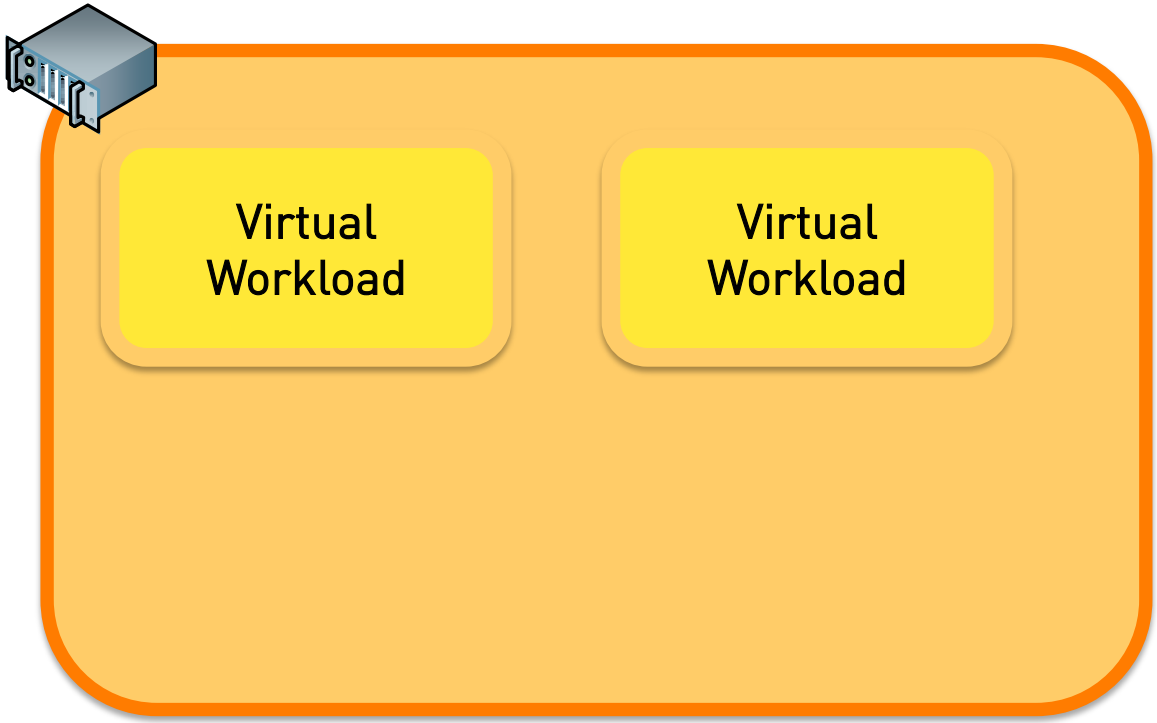




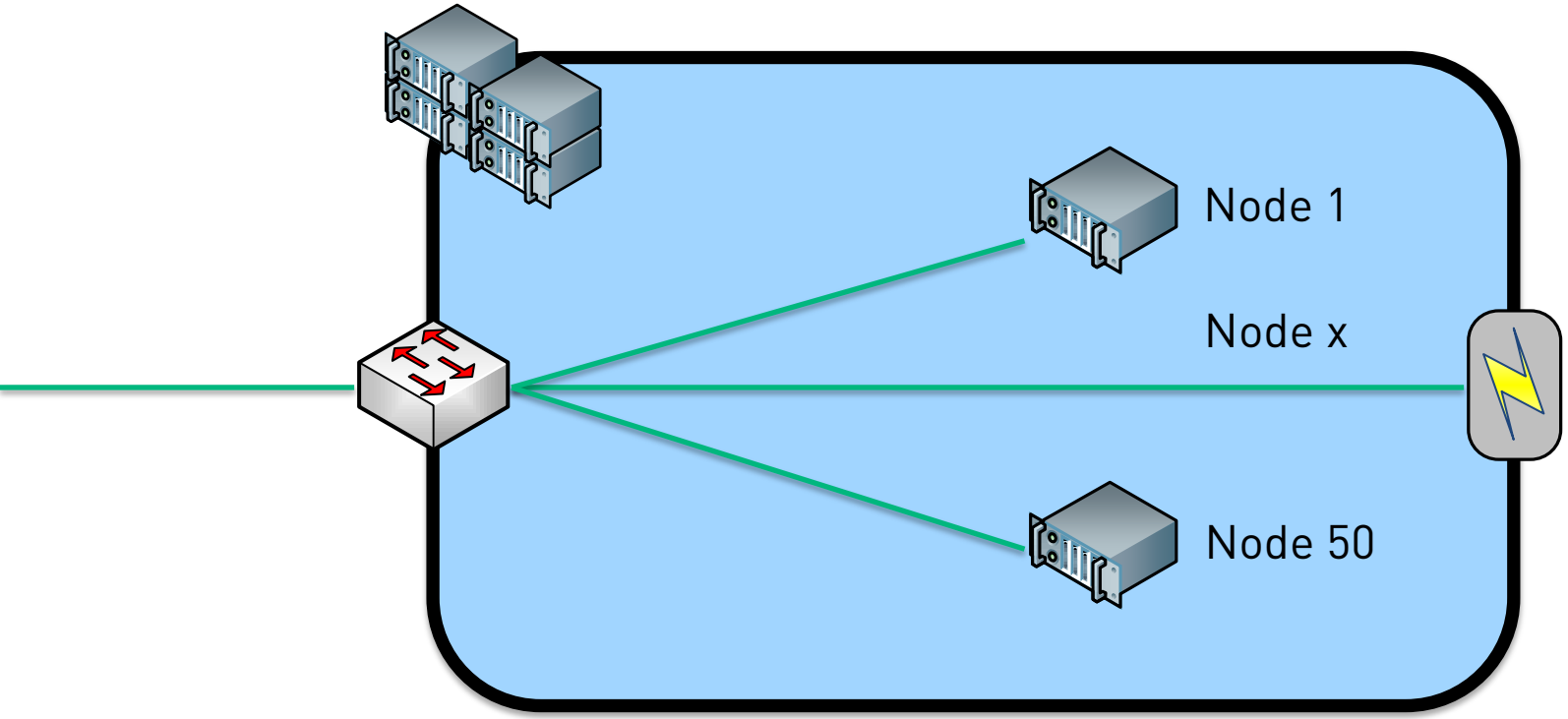
Workload

Virtual Workload

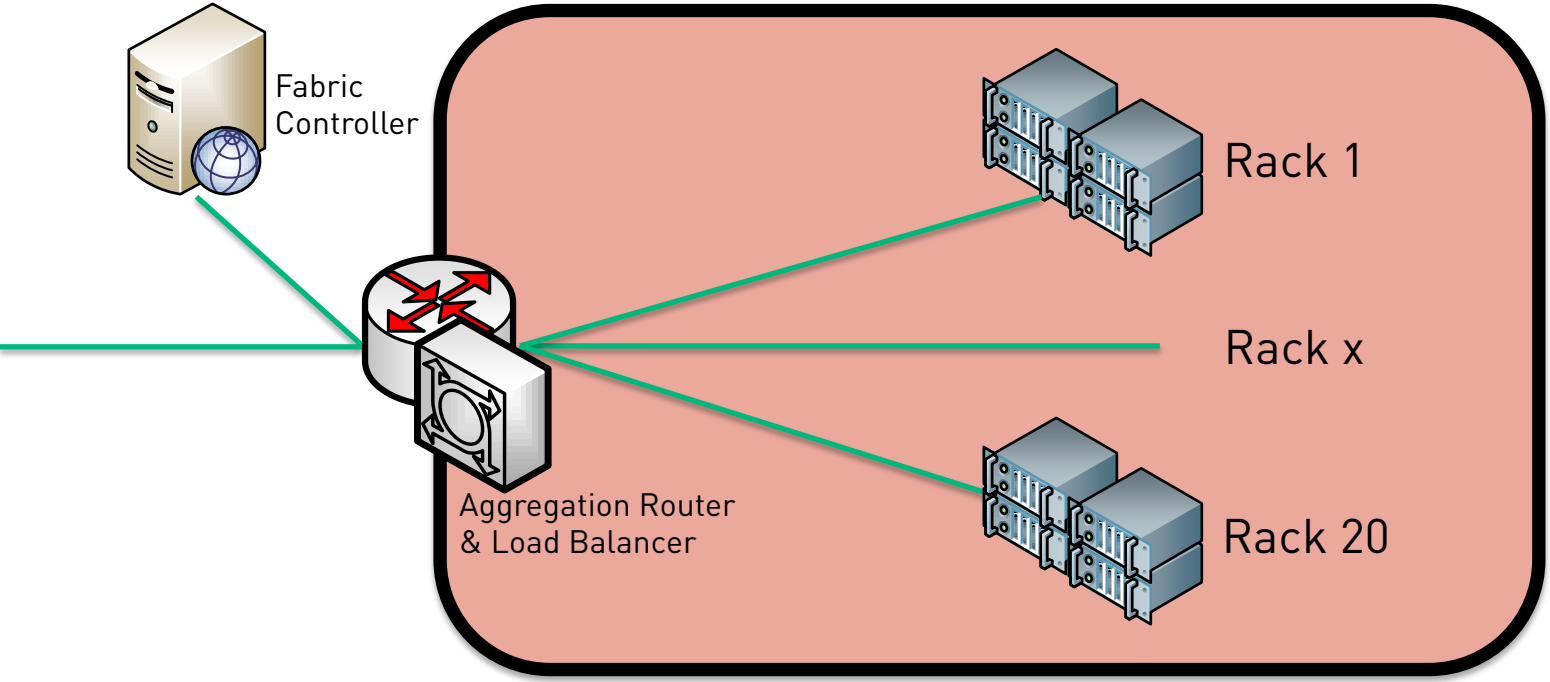
Compute Node



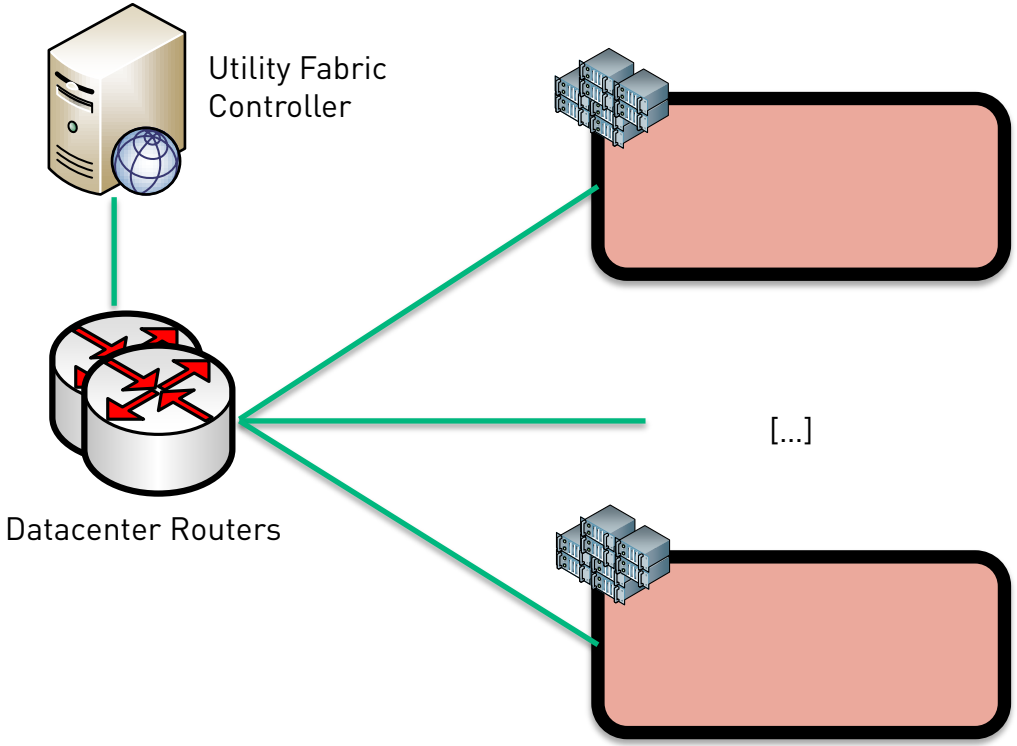
Rack



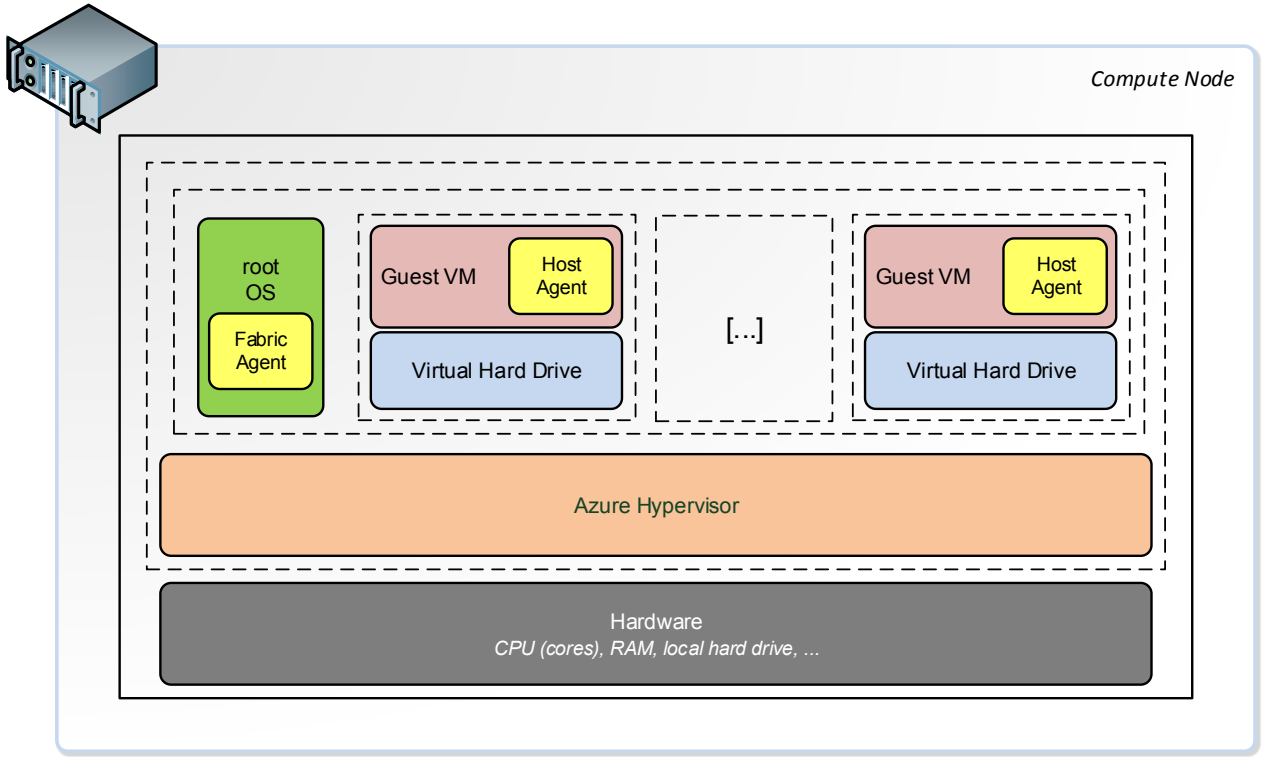
Cluster


Fabric Controller
Aggregation Router & Load Balancer
Rack 1
Rack x
Rack 20

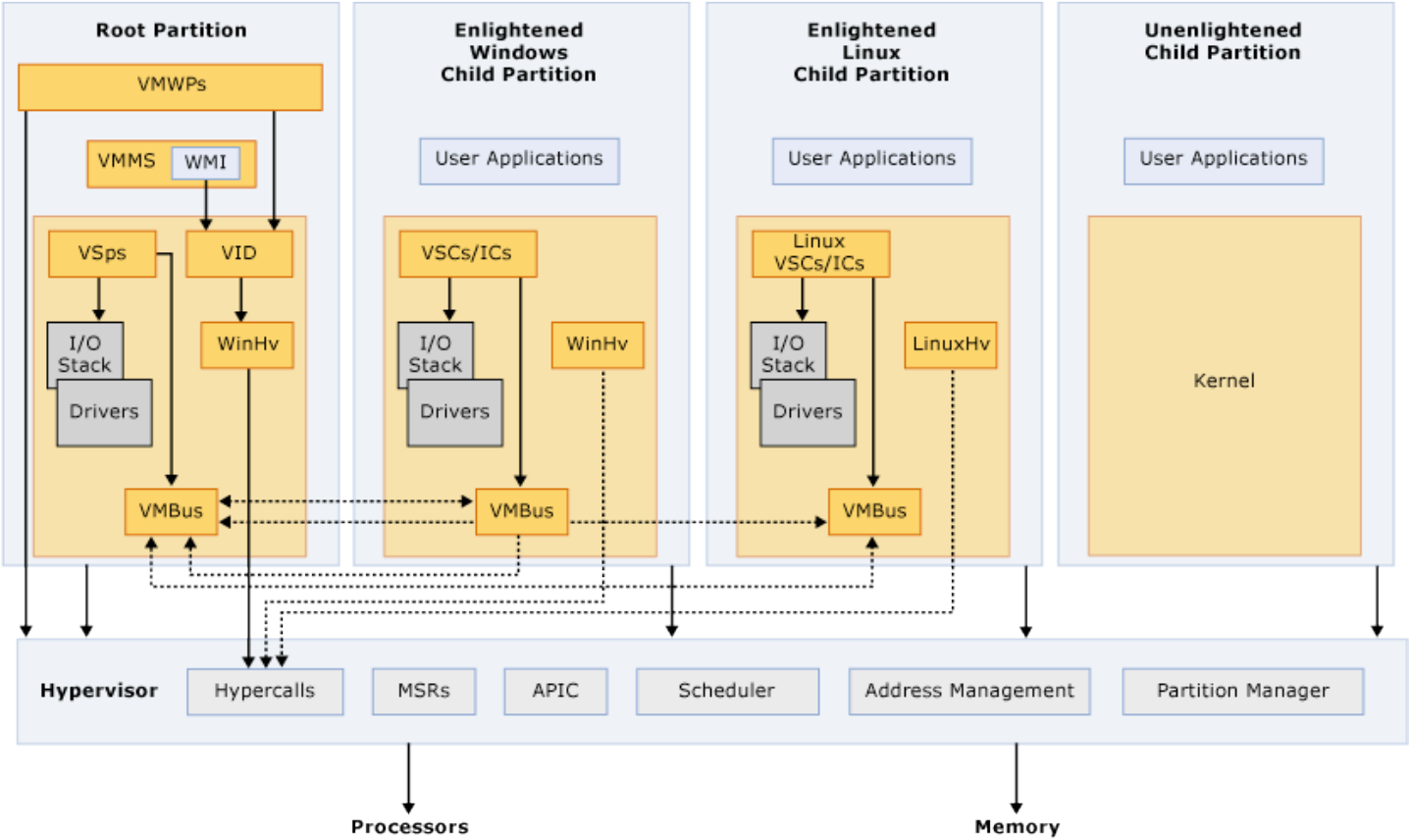
Fabric



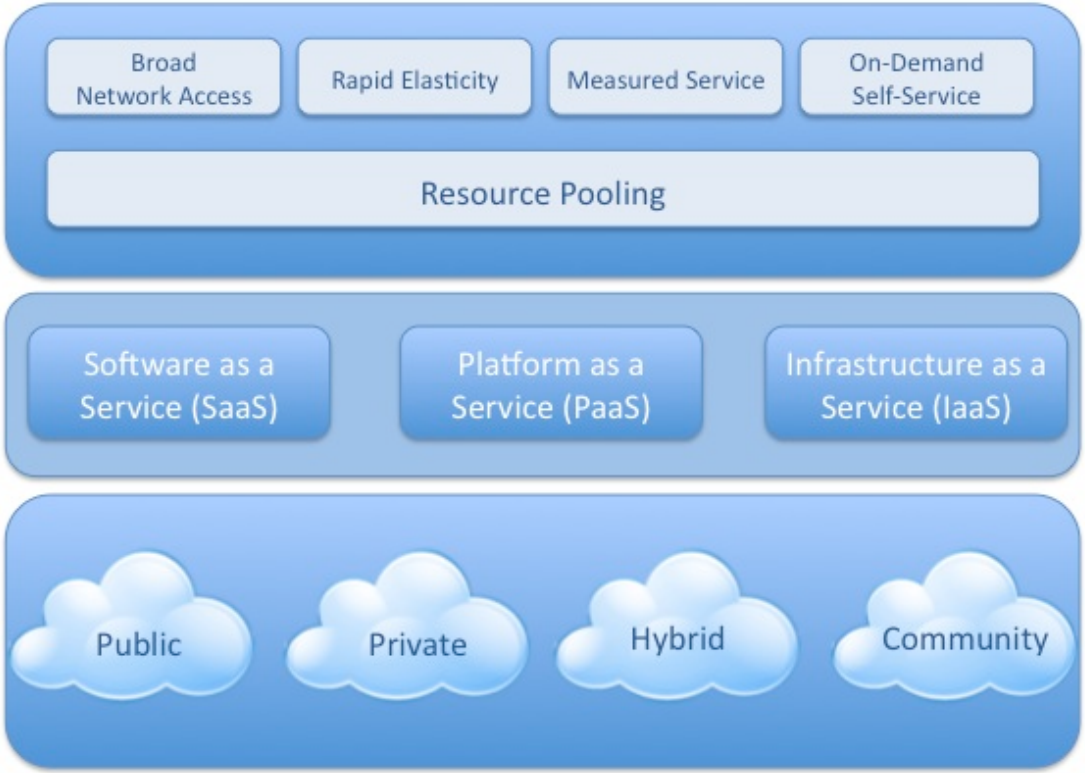
Compute Node



Hyper-V High Level Architecture



Source: http://msdn.microsoft.com/de-de/library/cc768520(en-us).aspx



Essential Characteristics

Service Models

Deployment Models

Definition of Cloud Computing

Main Cloud Risks

As of ENISA

R.1 LOCK-IN

Probability	HIGH	Comparative: Higher
Impact	MEDIUM	Comparative: Equal
Vulnerabilities	V13. Lack of standard technologies and solutions V46. Poor provider selection V47. Lack of supplier redundancy V31. Lack of completeness and transparency in terms of use	
Affected assets	A1. Company reputation A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery	
Risk	**HIGH**	

Lock-in

R.2 LOSS OF GOVERNANCE

Probability	VERY HIGH	Comparative: Higher
Impact	VERY HIGH (depends on organization) (IaaS VERY HIGH, SaaS Low)	Comparative: Equal
Vulnerabilities	V34. Unclear roles and responsibilities V35. Poor enforcement of role definitions V21. Synchronizing responsibilities or contractual obligations external to cloud V23. SLA clauses with conflicting promises to different stakeholders V25. Audit or certification not available to customers V22. Cross-cloud applications creating hidden dependency V13. Lack of standard technologies and solutions V29. Storage of data in multiple jurisdictions and lack of transparency about THIS V14. No source escrow agreement V16. No control on vulnerability assessment process V26. Certification schemes not adapted to cloud infrastructures V30. Lack of information on jurisdictions V31. Lack of completeness and transparency in terms of use V44. Unclear asset ownership	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery	
Risk	**HIGH**	

Loss of Governance

R.3 COMPLIANCE CHALLENGES

Probability	VERY HIGH – depends on PCI, SOX	Comparative: Higher
Impact	HIGH	Comparative: Equal
Vulnerabilities	V25. Audit or certification not available to customers V13. Lack of standard technologies and solutions, V29. Storage of data in multiple jurisdictions and lack of transparency about THIS V26. Certification schemes not adapted to cloud infrastructures V30. Lack of information on jurisdictions V31. Lack of completeness and transparency in terms of use	
Affected assets	A20. Certification	
Risk	**HIGH**	

Compliance Challenges

R.9 Isolation failure

Probability	LOW (Private Cloud) MEDIUM (Public Cloud)	Comparative: Higher
Impact	VERY HIGH	Comparative: Higher
Vulnerabilities	V5. Hypervisor vulnerabilities V6. Lack of resource isolation V7. Lack of reputational isolation V17. Possibility that internal (cloud) network probing will occur V18. Possibility that co-residence checks will be performed	
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery	
Risk	**HIGH**	

Isolation Failure

R.10 CLOUD PROVIDER MALICIOUS INSIDER - ABUSE OF HIGH PRIVILEGE ROLES

Probability	MEDIUM (Lower than traditional)	Comparative: Lower
Impact	VERY HIGH (Higher than traditional)	Comparative: Higher (aggregate) Comparative: Same (for a single customer)
Vulnerabilities	V34. Unclear roles and responsibilities V35. Poor enforcement of role definitions V36. Need-to-know principle not applied V1. AAA vulnerabilities V39. System or OS vulnerabilities V37. Inadequate physical security procedures V10. Impossibility of processing data in encrypted form V48. Application vulnerabilities or poor patch management	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A4. Intellectual property A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A9. Service delivery – real time services A10. Service delivery	
Risk	**HIGH**	

Malicious Insider

R.21 SUBPOENA AND E-DISCOVERY

Probability	HIGH
Impact	MEDIUM
Vulnerabilities	V6. Lack of resource isolation V29. Storage of data in multiple jurisdictions and lack of transparency about THIS V30 Lack of information on jurisdictions
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7 Personal data - critical A9. Service delivery – real time services A10. Service delivery
Risk	HIGH

Subpoena

R.22 Risk from changes of jurisdiction

Probability	VERY HIGH
Impact	HIGH
Vulnerabilities	V30. Lack of information on jurisdictions V29. Storage of data in multiple jurisdictions and lack of transparency about THIS
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery
Risk	HIGH

Changes of jurisdiction

R.23 DATA PROTECTION RISKS

Probability	HIGH
Impact	HIGH
Vulnerabilities	V30. Lack of information on jurisdictions V29. Storage of data in multiple jurisdictions and lack of transparency about THISthis
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery
Risk	HIGH

Data protection risks

And as of ERNW...

- ... Management Interfaces.
- Have a look at the Hacking Night School ;-)

http://www.rationalsurvivability.com/blog/?p=1836

You Can't Secure The Cloud…

April 30th, 2010 beaker Go to comments Leav

That's right. You can't secure "The Cloud" and the real shocker is that you don't need to.

You can and should, however, secure your assets and the elements within your control that are delivered by cloud services and cloud service providers, assuming of course there are interfaces to do so made available by the delivery/deployment model and you've appropriately assessed them against your requirements and appetite for risk.

That doesn't mean it's easy, cheap or agile, and lest we forget, just because you can "secure" your assets does not mean you'll achieve "compliance" with those mandates against which you might be

You can't secure the Cloud

Introduction to the Systems Operation Lifecycle

1. Hardware is purchased. . .
2. . . . from trusted hardware suppliers.
3. The hardware is operated in own data centers. . .
4. . . . which reside in carefully selected countries and locations. . .
5. . . . and are secured by carefully selected access control mechanisms.
6. The hardware is operated by trusted employees. . .
7. . . . who install operating systems. . .
8. . . . from trusted install media. . .
9. . . . in a secure, documented way...
10. ... and operate them in a secure, documented way.
11. The operating system is secured by carefully selected controls.
12. Only approved applications are installed. . .
13. . . . from trusted install media. . .
14. . . . and operated and secured using carefully developed guidelines.
15. Hosted applications are developed following carefully developed secure coding guidelines.

Mapping Risks

Risk	Step in Systems Operations Life Cycle
Lock-in	7-11
Loss of Governance	1-13
Compliance Challenges	1-13
Isolation Failure	1-13
Malicious Insider	3-6
Subpoena	4
Changes in Jurisdiction	4
Data Protection	1-13
Management Interfaces	1-10

Mapping Risks

Risk	Step in Systems Operations Life Cycle	Steps under control of (IaaS) CSP
Lock-in	7-11	7-9
Loss of Governance	1-13	1-9
Compliance Challenges	1-13	1-9
Isolation Failure	1-13	1-9
Malicious Insider	3-6	3-6
Subpoena	4	4
Changes in Jurisdiction	4	4
Data Protection	1-13	1-9
Management Interfaces	1-10	1-9

… and which of those are addressed by Devs?

Risk	Step in Systems Operations Life Cycle	Steps under control of (IaaS) CSP
Lock-in	7-11	7-9
Loss of Governance	1-13	1-9
Compliance Challenges	1-13	1-9
Isolation Failure	1-13	1-9
Malicious Insider	3-6	3-6
Subpoena	4	4
Changes in Jurisdiction	4	4
Data Protection	1-13	1-9
Management Interfaces	1-10	1-9

http://www.rationalsurvivability.com/blog/?p=1836

You Can't Secure The Cloud…

April 30th, 2010 beaker Go to comments Leav

That's right. You can't secure "The Cloud" and the real shocker is that you don't need to.

You can and should, however, secure your assets and the elements within your control that are delivered by cloud services and cloud service providers, assuming of course there are interfaces to do so made available by the delivery/deployment model and you've appropriately assessed them against your requirements and appetite for risk.

That doesn't mean it's easy, cheap or agile, and lest we forget, just because you can "secure" your assets does not mean you'll achieve "compliance" with those mandates against which you might be

You can't secure the Cloud

Azure Security

... Mechanisms

- Transport Encryption
- Network segmentation/isolation
- No vulnerability history
- Hardened systems
  - Both infrastructure and virtual machines

Transport Encryption

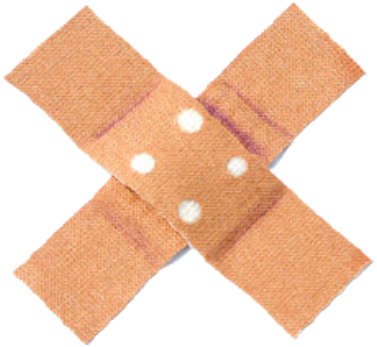
- All management traffic is SSL encrypted.
- Certificates are used for both client and server authentication
- SSL for applications can be configured as well.

Network Isolation

- 3 different network segments:
  - Fabric Controller
  - Infrastructure (e.g. network devices)
  - Untrusted (all hosted workloads)
- Isolation between segments
  - E.g. ACLs between Fabric Controller and Fabric Agents

Vulnerability History

... and Hardening



- No relevant vulnerabilities so far.
  - One DoS in HyperV
  - One vulnerability in the Azure SDK
- Template virtual machines hardened and patched...

Azure #Fails so far

- Two (Three ;)) outages
- CVE-2011-1068
- CVE-2011-1872

Microsoft Azure Leap Year Glitch

http://blogs.msdn.com/b/windowsazure/archive/2012/03/09/summary-of-windows-azure-service-disruption-on-feb-29th-2012.aspx

Overview

- Outage affected Azure Compute and dependent services (such as Access Control Service, Service Bus, SQL Azure Portal, Data Sync Services)
  - SQL Azure and Azure Storage was not impacted

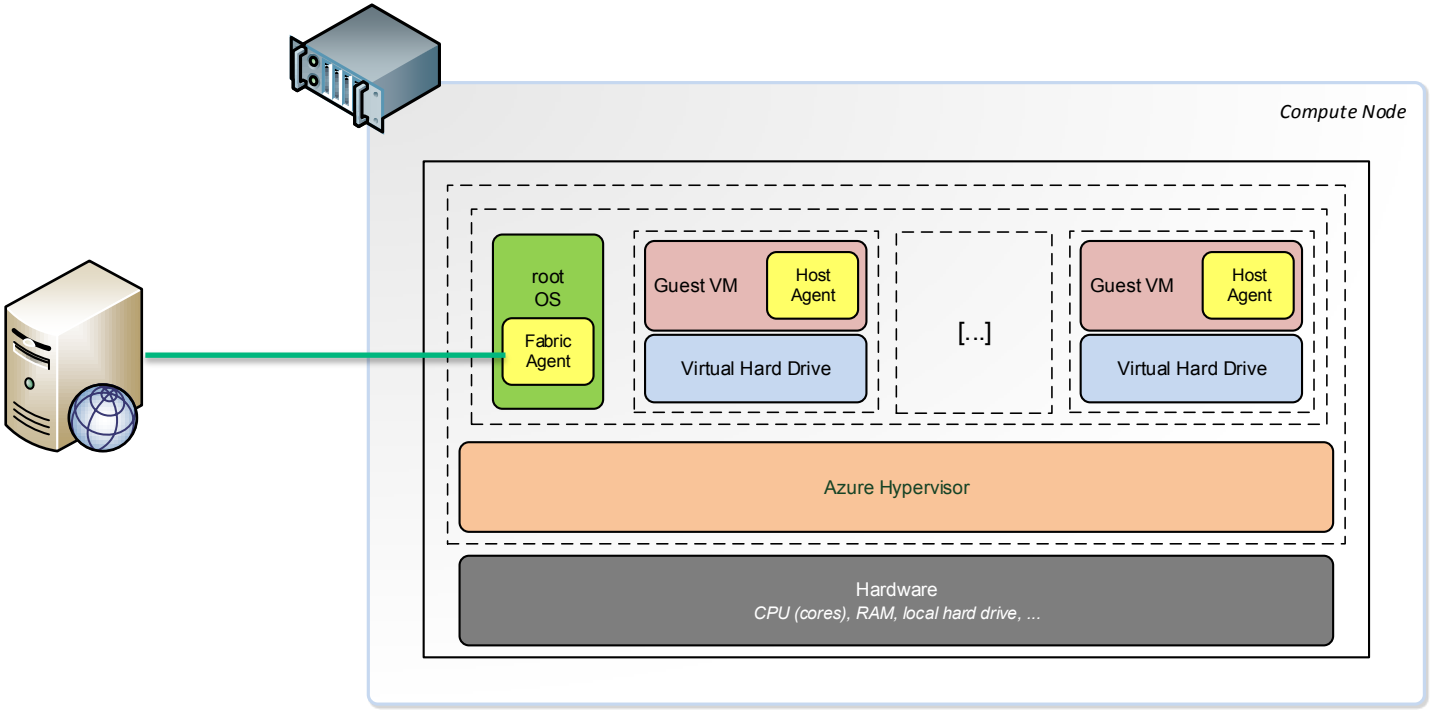
Azure Background

- Tight integration requires guest agents (GAs) and fabric agents (FAs) which the FC uses for interaction
- GAs for example generate a so-called transfer certificate when it is initialized. This allows the encrypted communication between FA and GA
- Transfer certificates are valid for one year.

Outage in one Sentence

- Certificates created on Feb 29 2012 had a validity until Feb 29 2013 – you see what they did there? ;-)
- Obviously, certificate generation failed due to an invalid *valid-to* date.
- Thus, the GA initialization fails (25 minute timeout to contact the HA)
- When the GA initialization fails, the VM is bootstrapped again
- If this bootstrapping fails three times, an hardware error is assumed ;-)

Compute Node



2nd Outage

http://blogs.msdn.com/b/windowsazure/archive/2012/08/02/root-cause-analysis-for-recent-windows-azure-service-interruption-in-western-europe.aspx

2nd Outage

- July 26 2012, 2 hours
- West Europe Sub-Region
- Azure network infrastructure is “limiting the scope of connections that can be accepted by our datacenter network hardware devices”

2nd Outage

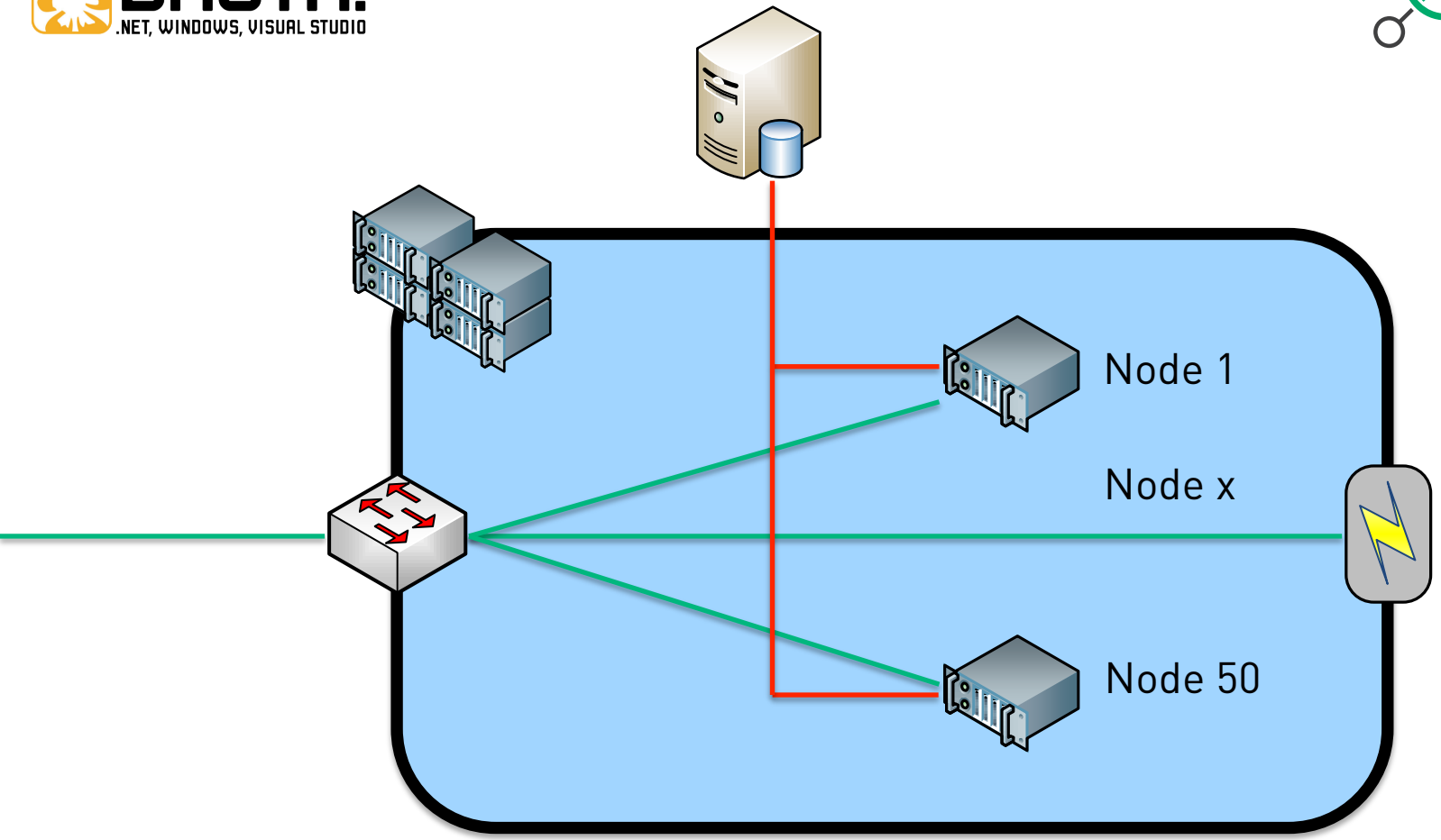
- Capacity upgrade was performed
- Infrastructure includes more devices = more endpoints
- “Scope” of connections wasn’t adjusted
- Significantly increased number of error messages, triggered bug.
- Human error was root cause!

Live News

3rd Outage on Feb 23 ;-)

Expired SSL Certificate

- SSL certificate of Azure Storage expired
- Started on Feb 23, 12:44 PM PST, services were restored to 99% worldwide by Feb 24, 1:00 AM PST
- No further details yet.


Node 1
Node x
Node 50

Cloud Impact

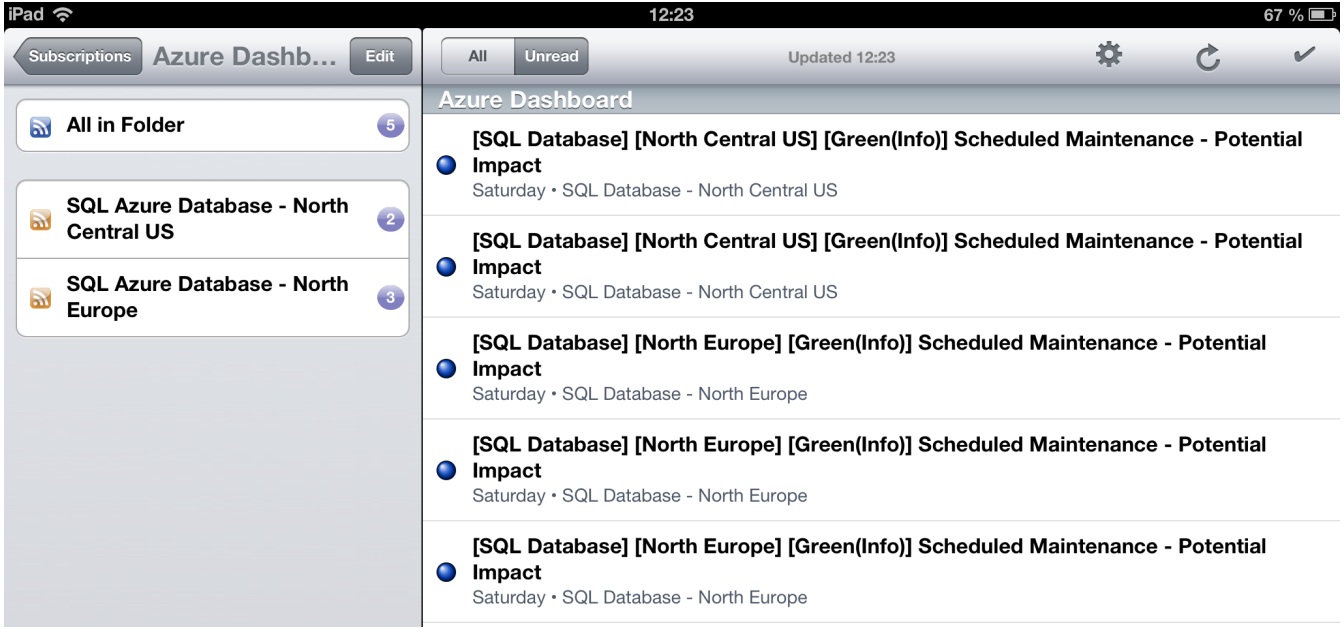
... for Developers

- No actual SLAs
- "We guarantee..." uptime of service X, but no refunds.
  - ;-)
  - Typically, service credits are granted.
- http://www.windowsazure.com/en-us/support/legal/sla/

Cloud Impact

... for Developers

¬ Scheduled Downtimes



Cloud Impact

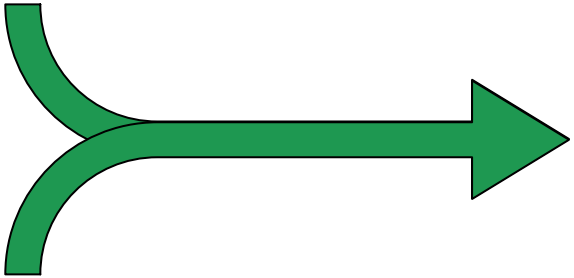
... for Developers

- Penetrationtests more difficult
- Only possible for own applications
- Is this enough...?
  - In order to assess this, you have to assess whether you want to *trust* your CSP.

- http://download.microsoft.com/download/C/A/1/CA1E438E-CE2F-4659-B1C9-CB14917136B3/Penetration%20Test%20Questionnaire.docx

In the end, you want to feel *confident*.

TRUST



CONFIDENCE

CONTROL

Potential Trust Metric

	Amazon WS	Azure	$SOME_SAAS
Symmetry	2	3	4
Transparency	1	3	4
Consistency	2	5	1
Integrity	2	4	2
Value of Reward	5	4	3
Components	4	3	2
Porosity	3	3	2
Trust Factor	**19**	**25**	**18**

Note: Sample Metric. Obviously, your assessment will vary.

Further Reading: http://www.insinuator.net/2011/06/broken-trust-part-1-definitions-fundamentals-some-more-reflections-on-rsa/

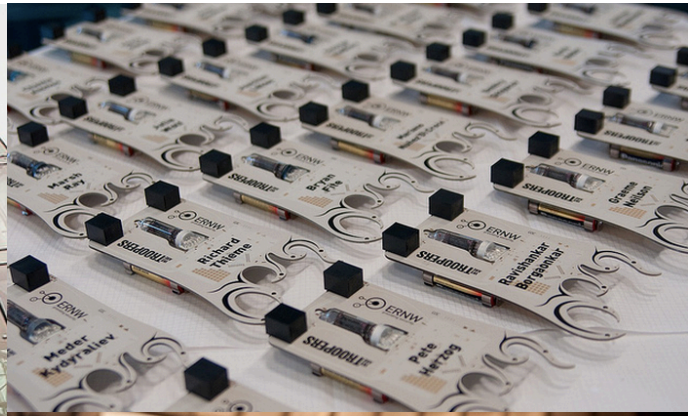
Remaining Risks

- Assess your assets.
  - And decide whether you want to put them in the cloud.
- Evaluate whether you want to *trust* the Cloud Service Provider.

Conclusions

- Azure has a good security posture so far.
- Intrinsic Cloud challenges remain.
- Adjust your security/threat models to the new cloud world.
  - Think in terms of the Systems Operations Life Cycle
  - Decide where you have to/want to trust your Cloud Service Provider
    - Document it!

Workshops, Conference, Roundtables, PacketWars Hacking Contest, 10k Morning Run, …



March
11th-15th 2013

Heidelberg,
Germany

www.troopers.de