

DEN
deutsches forschungsnetz





Erfahrungen bei Auswahl von Cloudlösungen für DFNconf

DFN Betriebstagung – GÉANT IaaS | 15.3.2018

Jürgen Hornung

Motivation für IaaS Einsatz

- Start einer neuen Videokonferenzplattform
- Wechsel von dedizierter Hardware zu virtualisierten Lösungen auf Standard Intel Servern
- Aufbau, Management und Wartung
- Keine Ausschreibung notwendig
- Breites Portfolio von Anbietern für VMware, KVM, MS-Azure, Amazon-AWS
- Alle Anbieter erfüllen Sicherheitsstandards, z.B. ISO27001

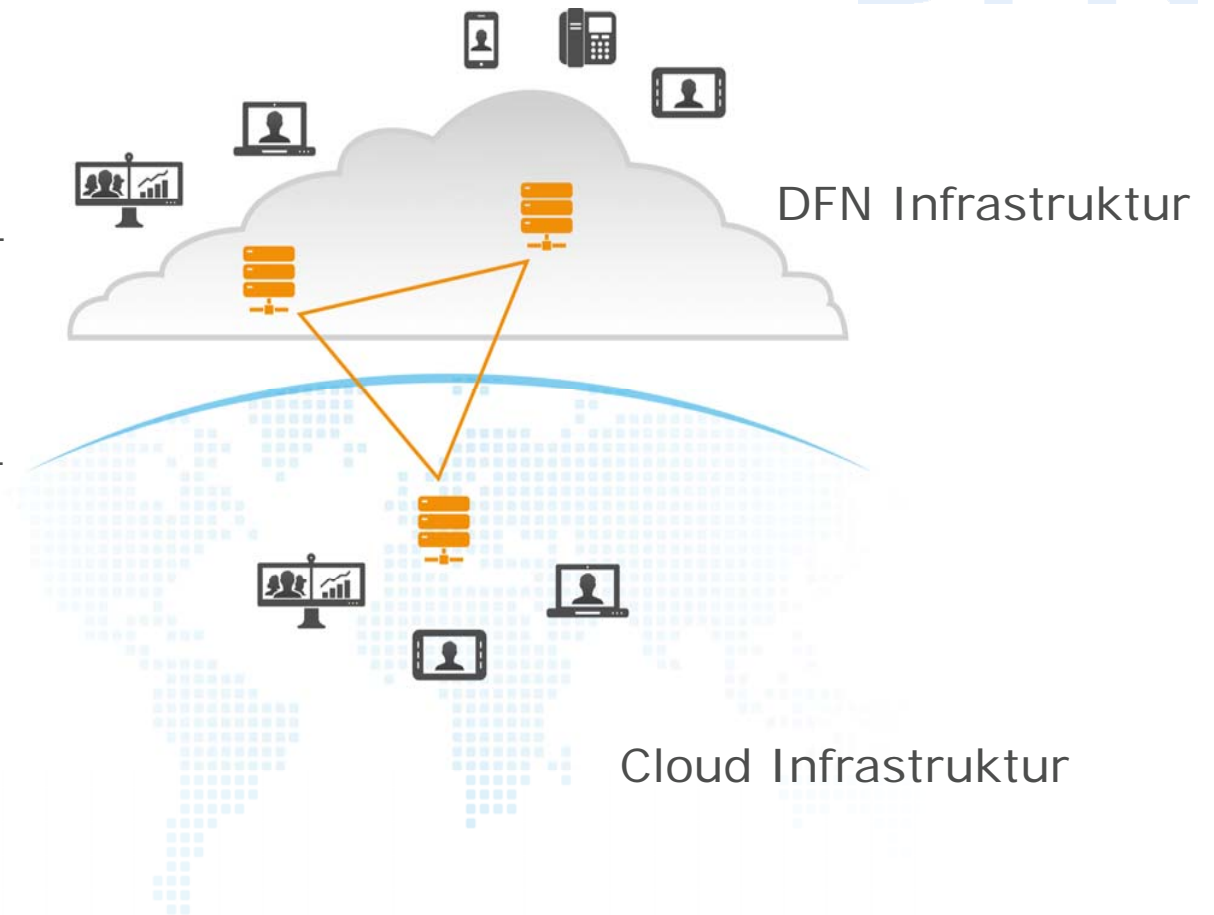


Aufgabenstellung (I)

DFN

Hybridmodell:

- Server (Management- und Konferenzserver) stehen an DFN-Kernnetzstandorten
 - Virtualisierung: VMware
- Server (Konferenzserver) stehen an Cloud-Standorten
 - Virtualisierung: VMware, (Amazon-AWS: *Sonderfall*)



Auswahl der Anbieter - Pflichtenheft

- Sicherheitsstandard: (Erfüllt durch GÉANT Ausschreibung)
- Virtualisierungslösung: VMware oder Amazon-AWS
AWS: Nur Bursting mit automatischem Serverstart ab definierter Lastgrenze
- Peering mit DFN
- „Echte“ Public-IP Adresse für Server, kein NAT
-> Bei keinem Anbieter möglich!
- VPN
-> IPsec bieten alle, laut Aussage von DFN-NOC aber Performanceprobleme ohne Hardwareunterstützung
- *Management/Monitoring in DFN-Infrastruktur*

Auswahl Anbieter (I): Dimension Data



+ Intuitiv zu bedienende Oberfläche

+ Gute Umsetzung von Server/Netzwerkconfiguration

+ Viele Möglichkeiten von lastabhängigen Hardware-scalings

o VMwareplattform nicht ersichtlich

- Kompatibilitätsprobleme beim Import von VMware-Images

The screenshot shows the Dimension Data CloudControl interface. At the top, it displays the user is logged in as 'juergen' with a 'Log Out' button. The main navigation bar includes 'Compute' and 'Cloud Backup' menus. Below this, there are filters for 'Europe' and 'DFNconf', and a search bar for 'Server / Network / Tag Search (Europe)'. The central area is titled 'DFNconf' and shows details for a network domain: 'Id: 00e8f5bb-bb3f-4a24-b066-e4a66031820e', 'Network Plan: Advanced', 'Data Center: Frankfurt (EU6)', 'Created: January 30, 2018', 'SNAT IPv4 Address: 168.128.10.32', and 'Outside Transit VLAN IPv4 Subnet: 100.64.2.0/28'. There are icons for 'Edit Network Domain', 'Manage Network Domain Tags', 'Delete Network Domain', and 'Deploy Server'. Below the details, there are two tables. The first table is 'Servers' with columns: Name, Services, Public IPv4, Primary IPv4, Primary IPv6, CPU, RAM, and Actions. It lists three servers: 'Conf-Node-1', 'ec_test_EU6_vertical', and 'Pexip-Management-Node'. The second table is 'VLANs and Servers' with columns: Name, IPv4 Range, IPv6 Range, and Actions. It lists one entry: 'pexip MCU'.

Name	Services	Public IPv4	Primary IPv4	Primary IPv6	CPU	RAM	Actions
Conf-Node-1		168.128.12.158	192.168.0.20	2a00:47c0:111:1194:8ea:516:32d5:d089	6 CPU	6 GB	
ec_test_EU6_vertical			192.168.0.6	2a00:47c0:111:1194:184f:92ce:4ce5:f01d	2 CPU	4 GB	
Pexip-Management-Node		168.128.12.16	192.168.0.16	2a00:47c0:111:1194:4f0f:8cdf:f235:693f	1 CPU	4 GB	

Name	IPv4 Range	IPv6 Range	Actions
pexip MCU	192.168.0.0 /24	2a00:47c0:111:1194:0:0:0 /64	

Auswahl Anbieter (I): Dimension Data



+ Intuitiv zu bedienende Oberfläche

+ Gute Umsetzung von Server/Netzwerkkonfiguration

+ Viele Möglichkeiten von lastabhängigen Hardware-scalings

o VMwareplattform nicht ersichtlich

- Kompatibilitätsprobleme beim Import von VMware-Images

Firewall Rules									Actions
Firewall Rules			IP Address Lists		Port Lists				
	Name	Protocol	Source		Destination		Action		
			IP Address	Port	IP Address	Port			
✓	CCDEFAULT.BlockOutb	TCP	ANY	Any	ANY	25	⊘	⚙	
✓	CCDEFAULT.BlockOutb	TCP	ANY	Any	ANY	587	⊘	⚙	
✓	CCDEFAULT.BlockOutb	TCP	ANY	Any	ANY	25	⊘	⚙	
✓	CCDEFAULT.BlockOutb	TCP	ANY	Any	ANY	587	⊘	⚙	
✓	CCDEFAULT.DenyExtern	IP	EXTERNAL_IPV6	Any	ANY	Any	⊘	⚙	
✓	! Allow_ICMP	ICMP	ANY	Any	ANY	Any	✓	⚙	
✓	Allow.All.from.DFNVC.N	IP	194.95.240.0 / 24	Any	168.128.12.16	Any	✓	⚙	
✓	Allow.https.access.to.F	TCP	ANY	Any	168.128.12.16	443	✓	⚙	
✓	http.access..conf.node	TCP	ANY	Any	168.128.12.158	80	✓	⚙	
✓	https.access..conf.nod	TCP	ANY	Any	168.128.12.158	443	✓	⚙	
✓	h225.access..conf.nod	TCP	ANY	Any	168.128.12.158	1720	✓	⚙	
✓	sip.s.access..conf.nod	TCP	ANY	Any	168.128.12.158	5060 - 5061	✓	⚙	
✓	signal.access..conf.noc	TCP	ANY	Any	168.128.12.158	33000 - 34000	✓	⚙	
✓	media.access..conf.noc	TCP	ANY	Any	168.128.12.158	40000 - 41000	✓	⚙	

Auswahl Anbieter (I): Dimension Data



+ Intuitiv zu bedienende Oberfläche

+ Gute Umsetzung von Server/Netzwerkconfiguration

+ Unterschiedliche Möglichkeiten des lastabhängigen VM-Scalings

o VMwareplattform nicht ersichtlich

- Kompatibilitätsprobleme beim Import von VMware-Images

The screenshot displays the Dimension Data Auto Scaling Manager interface. A modal window titled "Create New Vertical Auto Scaling Rule" is open, containing the following fields and values:

- Network / Network Domain: EU6/DFNconf
- Server: EU6/ec_test_EU6_vertical
- Metric: CPU
- Auto Scaling Thresholds: 10 to 80
- Amount of Time Before Up Scaling: 15 minutes
- Amount of Time Before Down Scaling: 1 hour
- Auto Scaling Increments: (empty)

The background interface shows the "Auto Scaling Manager" dashboard with sections for "Horizontal Auto Scaling Rules", "Vertical Auto Scaling Rules", and "Recent Auto Scaling Actions (Last 10)". The user is logged in as "juergen".

Auswahl Anbieter (I): Dimension Data



+ Intuitiv zu bedienende Oberfläche

+ Gute Umsetzung von Server/Netzwerkconfiguration

+ Viele Möglichkeiten von lastabhängigen Hardware-scalings

o VMwareplattform nicht ersichtlich

- Kompatibilitätsprobleme beim Import von VMware-Images

The screenshot shows the Dimension Data CloudControl interface. At the top, there's a navigation bar with 'Compute' and 'Cloud Backup' tabs. Below that, a search bar contains 'Server / Network / Tag Search (Europe)'. The main content area displays the 'DFNconf' network configuration. On the left, there are several action buttons: 'Edit Network Domain', 'Manage Network Domain Tags', 'Delete Network Domain', 'Deploy Server', and 'Data Center VPN'. The main configuration area shows the following details:

- DFNconf**
Id: 00e8f5bb-bb3f-4a24-b066-e4a66031820e
Network Plan: Advanced
- Data Center:** Frankfurt (EU6)
Created: January 30, 2018
SNAT IPv4 Address: 168.128.10.32
Outside Transit VLAN IPv4 Subnet: 100.64.2.0/28
Tags:

Below this, there are two tables:

Servers							
Name	Services	Public IPv4	Primary IPv4	Primary IPv6	CPU	RAM	Actions
Conf-Node-1	[Icons]	168.128.12.158	192.168.0.20	2a00:47c0:1111:1194:8ea:516:32d5:d089	6 CPU	6 GB	[Settings]
ec_test_EU6_vertical	[Icons]		192.168.0.6	2a00:47c0:1111:1194:184f:92ce:4ce5:f01d	2 CPU	4 GB	[Settings]
Pexip-Management-Node	[Icons]	168.128.12.16	192.168.0.16	2a00:47c0:1111:1194:4f0f:8cdf:f235:693f	1 CPU	4 GB	[Settings]

VLANs and Servers		
Name	IPv4 Range	IPv6 Range
pexip MCU	192.168.0.0 /24	2a00:47c0:1111:1194:0:0:0 /64

Auswahl Anbieter (II): T-Systems vCloud

+ VMware typische Oberfläche

o Relativ alte VMware Version (5.5)

o Server-/ Netzwerk-konfiguration jeweils eigene Oberflächen (Flash/HTML5)

o vCloud lässt sich via Plugin in eigene VMware Infrastruktur einbinden

o Schwierigkeiten beim Import von VMware Images

- Eingeschränkte Skalierungsmechanismen

The screenshot displays the VMware vCloud interface for GEANT LIMITED (0007178267)_1000027983. The user is logged in as 'jh (Organization Administrator)'. The interface shows a navigation menu on the left with 'My Cloud' selected, containing 'vApps', 'VMs', 'Expired Items', and 'Logs'. The main area is titled 'Pexip Conferencing Node Running' and shows a 'vApp Diagram' with a 'Pexip Management Node' and a 'Pexip Conferencing Node'. A virtual machine named 'pexip amd64' is connected to a 'VM Network' and a 'DFNConf' network. The status bar at the bottom indicates '0 Running' and '0 Failed' VMs, and is powered by VMware.

Auswahl Anbieter (II): T-Systems vCloud



+ VMware typische Oberfläche

o Relativ alte VMware Version (5.5)

o Server-/ Netzwerk-konfiguration jeweils eigene Oberflächen (Flash/HTML5)

o vCloud lässt sich via Plugin in eigene VMware Infrastruktur einbinden

o Schwierigkeiten beim Import von VMware Images

- Eingeschränkte Skalierungsmechanismen

The screenshot shows the vCloud Director interface for configuring NAT rules on an Edge-Gateway. The page title is "Edge-Gateway - com-a-gea_1000027983-01-gw01". The "NAT" tab is selected, showing a list of NAT rules. The table below details these rules:

ID	Typ	Aktion	Angewendet a...	Ursprünglich		Übersetzt		Protokoll	Aktivi...	Protokollierung	Beschreibung
				IP-Adresse	Port	IP-Adresse	Port				
196609	Benutzerdefiniert	SNAT	vm-vi3718-dsi-vcd	0.0.0.1-255.255.2	Beliebig	6.204.73.13	Beliebig	Beliebig	✓	✗	T-SYSTEMS Service Zone Source...
196621	Benutzerdefiniert	SNAT	vm-vi3720-dsi-vcc	192.168.11/24	Beliebig	80.158.12.178	Beliebig	Beliebig	✓	✗	
196620	Benutzerdefiniert	DNAT	vm-vi3720-dsi-vcc	80.158.12.178	8443	192.168.1.55	443	tcp	✓	✗	https Zugriff auf Management Node
196622	Benutzerdefiniert	DNAT	vm-vi3720-dsi-vcc	80.158.12.178	443	192.168.1.60	443	tcp	✓	✗	https Zugriff auf Conf Node
196623	Benutzerdefiniert	DNAT	vm-vi3720-dsi-vcc	80.158.12.178	8444	192.168.1.60	8443	tcp	✓	✗	API Zugriff auf Conf Node

Auswahl Anbieter (II): T-Systems vCloud

+ VMware typische Oberfläche

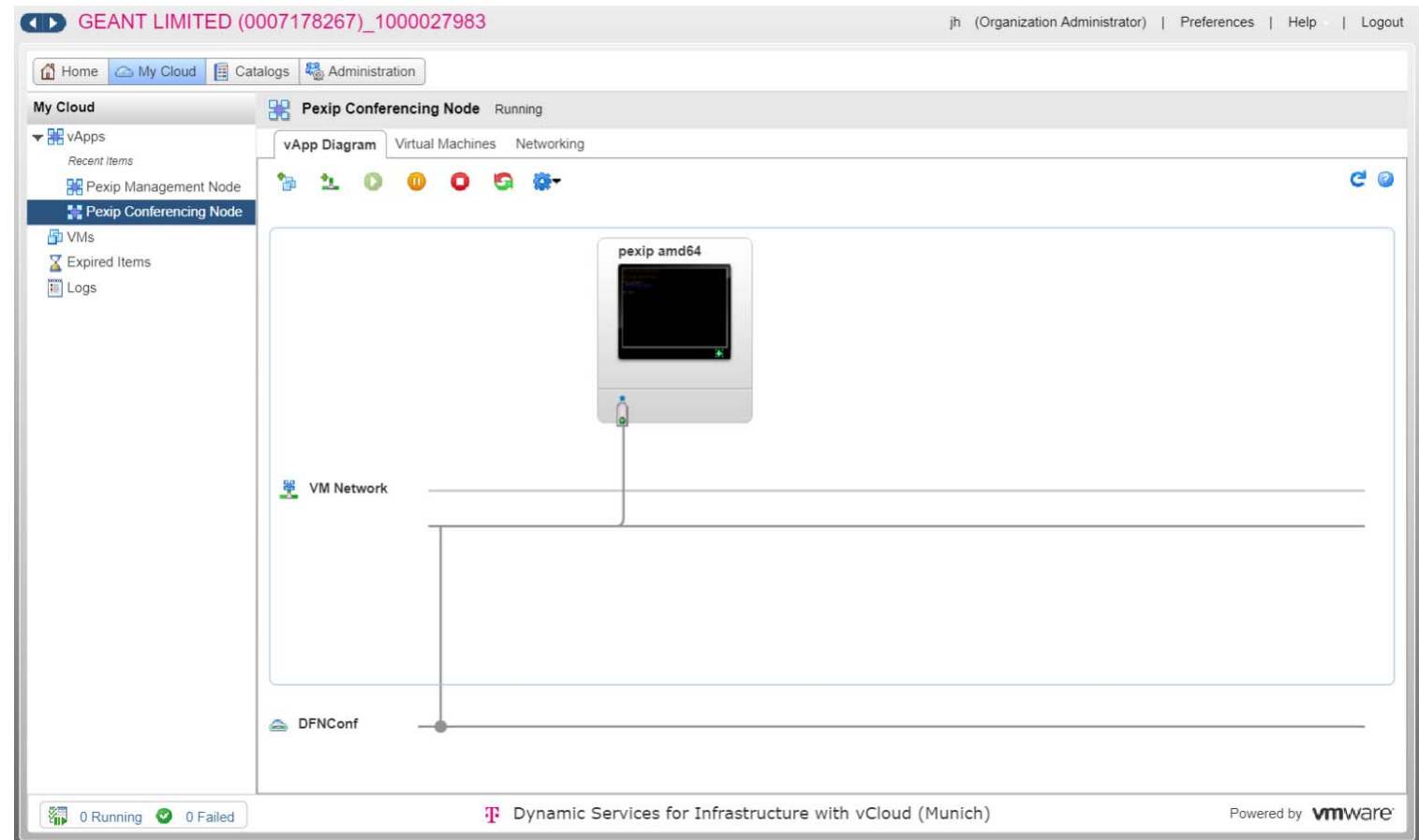
o Relativ alte VMware Version (5.5)

o Server-/ Netzwerk-konfiguration jeweils eigene Oberflächen (Flash/HTML5)

o vCloud lässt sich via Plugin in eigene VMware Infrastruktur einbinden

o Schwierigkeiten beim Import von VMware Images

- Eingeschränkte Skalierungsmechanismen



Auswahl Anbieter (III): Amazon AWS



+ Umfangreichstes Angebot
-> Zeitintensive Einarbeitung

o Keine Konfiguration von Hardwareparametern
-> AWS stellt Liste von unterschiedlichen VMs bereit

o Fremd VMs müssen importiert werden
-> Gefahr von Kompatibilitätsproblemen

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
Pexip ConfN...	i-05d66929edc6d6139	c4.2xlarge	eu-central-1a	stopped		None	ec2-18-196-190-250.eu...	18.196.190.250

Instance: i-05d66929edc6d6139 (Pexip ConfNode) Elastic IP: 18.196.190.250			
Description	Status Checks	Monitoring	Tags
Instance ID	i-05d66929edc6d6139		
Instance state	stopped		
Instance type	c4.2xlarge		
Elastic IPs	18.196.190.250*		
Availability zone	eu-central-1a		
Security groups	default, view inbound rules		
Scheduled events	-		
AMI ID	Pexip Infinity Conferencing Node 17.1.0 (build 40171.0.0) (ami-f9c75496)		
Platform	-		
IAM role	-		
Key pair name	Pexip_Conf_Node		
EBS-optimized	True		
Root device type	ebs		
Public DNS (IPv4)	ec2-18-196-190-250.eu-central-1.compute.amazonaws.com		
IPv4 Public IP	18.196.190.250		
IPv6 IPs	-		
Private DNS	ip-172-31-19-150.eu-central-1.compute.internal		
Private IPs	172.31.19.150		
Secondary private IPs	-		
VPC ID	vpc-049a3e6f		
Subnet ID	subnet-dd5d34b6		
Network interfaces	eth0		
Source/dest. check	True		
T2 Unlimited	-		
Owner	673571795847		
Launch time	February 12, 2018 at 2:39:55 PM UTC+1 (607 hours)		
Termination protection	True		

Zusammenfassung

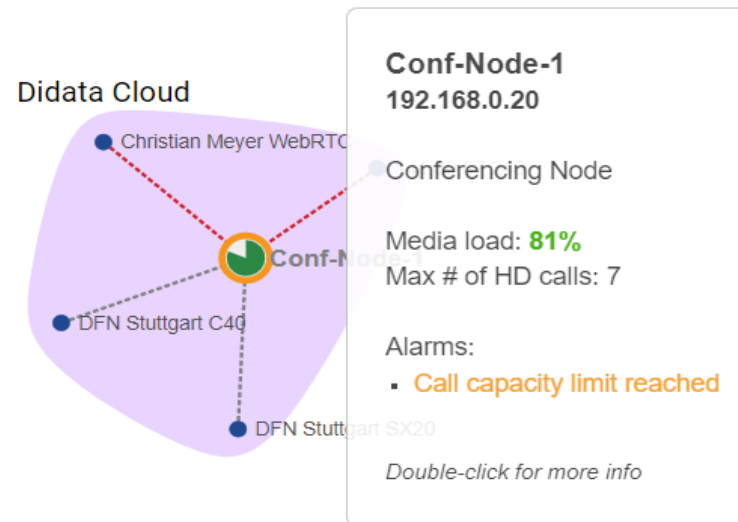
„Stolpersteine“ bei unseren Tests:

- Kein Anbieter unterstützt Public-IP Adressen, es kommt immer NAT zum Einsatz -> Wir konnten unser geplantes Hybrid-Modell ohne VPN nicht testen.
- VMware Images wurden oft fehlerhaft importiert: VM startete nicht, kein Autoscaling, fehlende Netzwerkinterfaces.
- Skalierungsmöglichkeiten bei Lastschwankungen vielfach ungenügend, entweder läuft die CPU nur mit geringer maximaler Taktfrequenz oder die dynamische Zuschaltung von zusätzlichen Kernen erfordert zu viel Zeit.
- Je nach Anbieter wochenlange Wartezeit, bis Testplattform zur Verfügung stand.

Zusammenfassung

„Stolpersteine“ bei unseren Tests:

- Kein Anbieter unterstützt Public-IP Adressen
Wir konnten unser geplantes Hybrid-Multicast-Setup nicht realisieren.
- VMware Images wurden oft fehlerhaft erstellt
fehlende Netzwerkinterfaces.
- Skalierungsmöglichkeiten bei Lastschwankungen vielfach ungenügend, entweder läuft die CPU nur mit geringer maximaler Taktfrequenz oder die dynamische Zuschaltung von zusätzlichen Kernen erfordert zu viel Zeit.
- Je nach Anbieter wochenlange Wartezeit, bis Testplattform zur Verfügung stand.



Fazit

- Möglichst genaues und umfangreiches Pflichtenheft hilft vor unangenehmen Überraschungen.
- Fragen Sie detailliert über die technischen Möglichkeiten nach, im Idealfall sollte ein Techniker bei den Gesprächen dabei sein.
- Vereinbaren Sie einen Zeitraum für eine Testinstallation.
- Einsatz für DFNconf auf Grund der aufgetretenen Probleme zur Zeit nicht praktikabel. Für die Zukunft sind aber weitere Tests für ein Hybrid Modell geplant.

Haben Sie noch Fragen?

