“V” FOR “VERY SECURE”

Dynamic Services for Infrastructure with vCloud

SECURITY IN THE CLOUD

T-Systems’ Dynamic Services for Infrastructure with vCloud (DSI vCloud) is a highly secure IaaS offering that enables businesses to scale their infrastructure resources up or down in line with demand. Users can leverage VMware technology to add virtual data centers to existing internal resources. Customers benefit from access to VMware interfaces and tools – which are widely used and trusted by data center operators. DSI vCloud is primarily delivered from twin-core data centers based in Germany. However, users can also request delivery from other sites around the globe. Moreover, DSI vCloud offers year-round availability of up to 99.98 percent – meaning that it is also an ideal choice for operating production environments.

The scope of service includes backup functions, managed operating systems, secure Internet access and disaster-recovery capabilities. As a result, the solution meets even the most exacting data availability and business continuity needs. All access paths are encrypted, while detailed logs support security audits and help organizations ensure compliance with complex requirements.

KEY SECURITY BENEFITS AT A GLANCE

LEADING-EDGE TECHNOLOGY

- Infrastructure in secure T-Systems twin-core data centers
- Redundancy of all DSI vCloud components
- Network isolation: dedicated firewalls, secure WAN connections, and dedicated customer-specific networks
- Segregation of customers at the level of network, compute and storage resources
- Robust protection for all external communication connections
- Encrypted, authenticated vCloud Management front end / API
- Internet access to virtual machines via firewall instances
- Administration of DSI vCloud via internal provider connections
- Penetration testing performed to verify high level of security
- Security and compliance logging and monitoring
- Web Application Firewall safeguards the security of vCloud Director

RELIABLE PROCESSES

- External and internal security and quality checks
- Data processed in line with German and European data protection legislation
- Identity and access management
- Security management processes

T · · Systems ·

WHAT MAKES vCLOUD SO SECURE?

NETWORK INFRASTRUCTURE. DSI vCloud leverages standardization and virtualization for network design, which means:

- Separation of networks (service, Internet, intranet and management zones)
- Implementation of demilitarized zones
- Decoupling through security gateways (web application firewalls, load balancers, reverse proxies, etc.)
- Logical separation of clients at network level on the basis of virtual networks

INTEGRATION. There are two ways of connecting to the cloud management portal. The first option is an Internet-based, hybrid cloud model (DSI vCloud Hybrid), while the alternative – a virtual private cloud model (DSI vCloud Private) – uses exclusively private network connections. MPLS, Ethernet Connect and IP-VPN must be ordered separately. Access to the DSI vCloud and the corresponding resources is managed using pre-defined roles and rights. Customers log on to their networks via a firewall cluster with a dedicated virtual firewall. Network traffic is segregated by means of zones, with each zone allocated to a single client and comprising one or more VLANs. It is possible to grant broader access over the Internet to applications or virtual machines on the customer's DSI vCloud network, via the DMZ and Internet firewall. Customers who use this option receive an additional network segment protected by a virtual firewall instance (vShield Edge).

STORAGE. In the DSI vCloud, storage resources are shared between several customers, who are strictly separated from one another. Storage is provisioned virtually via the hypervisor – preventing direct access to the system. Moreover, T-Systems encrypts the physical hard drives for additional security.

SECURITY MONITORING. Rigorous monitoring of DSI vCloud infrastructure systems, and of the optional operating systems managed by T-Systems, is ensured with tools and alerts such as:

- **Tivoli Module ONSEC:** for authentication and authorization
- **SIUX System Scanner and WinAudit:** compare operating system configurations (UNIX / Linux, Windows) with security standards
- **Antivirus:** antivirus software delivers warnings and alerts, and provides active protection for Windows operating systems
- The DSI vCloud Self-Service Portal, accessible over the Internet is regularly checked for potential vulnerabilities

TESTING. From the very beginning, DSI vCloud has been subjected to internal and external penetration testing, load tests and functional testing. Positive results have demonstrated that the platform is capable of reliably supporting multi-tenancy. The assessment revealed that there were no weaknesses that may allow unauthorized access to other customers' data.

LOGGING. DSI vCloud features automatic logging of changes to selected components to ensure complete transparency at all times.

CLEARLY DEFINED RESPONSIBILITIES. The customer has total control over their virtual machines (VM) and is responsible for ensuring that all VMs are protected in accordance with their specific security needs. This includes, for example, backing up VMs, data encryption within VMs, and integration of identity management and patch management systems. Self-service disaster recovery for DSI vCloud is an optional service.

RECOMMENDATIONS. In order to increase security for the customer, the following features are available and recommended for DSI vCloud:

- Account and rights management in vCloud Director
- Use of secure network protocols
- Definition of firewall rules based on whitelists
- Internal vCloud applications segregated into separate tiers through logical networks
- Backup of virtual machines using a backup-as-a-service (BaaS) solution (included; usage optional)
- Highly secure authentication protects all systems connected to the Internet or used for system administration

T-SYSTEMS STANDARDS. T-Systems operates Enterprise Security Architecture for Reliable ICT Services (ESARIS), an enterprise architecture for information security. It defines standard methodologies, processes and requirements for risk management and certification, evidence and customer relationship management, service management, customers / users, networks and data centers. The standards are based on ISO 27001, ITIL and other industry norms. Internal T-Systems standards form part of the certified information security management system.

T-SYSTEMS HAS ACHIEVED CORPORATE CERTIFICATION TO THE FOLLOWING STANDARDS:

- DIN EN ISO 9001: Quality management systems
- ISO/IEC 20000: IT Service Management (ITILv3)
- ISO/IEC 27001: Information technology security management systems
- ISO 14001: Environmental management
- OHSAS 18001: Certification for occupational health and safety
- ISAE 3402: International standards on assurance engagements

FURTHER INFORMATION
Internet: http://cloud.t-systems.com/solutions/dsi-vcloud

CONTACT
Heiko Röhr
Director of Sales, VMware
Phone: +49 40 306005173
Email: DSI@t-systems.com

PUBLISHED BY
T-Systems International GmbH
Hahnstr. 43d
60528 Frankfurt am Main
Germany