Windows Azure™ Security im Überblick

Von Charlie Kaufman und Ramanathan Venkatapathy

Zum Inhalt

Windows Azure muss als Plattform für Cloud Services die *Vertraulichkeit,* die *Integrität* und die *Verfügbarkeit* von Kundendaten sicherstellen. Darüber hinaus muss für den Kunden und für Microsoft stets transparent sein, wer welche Services administriert.

Dieses Dokument beschreibt die Sicherungs- und Steuerungsmechanismen von Windows Azure. Sie können als Kunden so besser einschätzen, ob diese Mechanismen zu Ihren individuellen Anforderungen passen. Der Überblick beginnt mit technischen Erläuterungen der Sicherheitsfunktionalitäten, die Kunden und Microsoft für den Betrieb von Windows Azure zur Verfügung stehen. Dazu zählen unter anderem

- Identity- und Accessmanagement über die Windows Live ID mit erweiterter SSL-Authentifizierung,
- Umgebungs- und Komponentenisolation auf mehreren Ebenen,
- Snapshots virtueller Maschinen und Integritätsprüfung der Konfiguration
- dreifach replizierter Storage zur Minimierung der Auswirkungen von Hardwarefehlern.

Darüber hinaus wird aufgezeigt, wie Monitoring, Protokoll- und Reportingfunktionen in Windows Azure für Transparenz in der Cloud-Umgebung des Kunden sorgen.

Im Anschluss an die technischen Erläuterungen befasst sich dieses Dokument mit den Menschen und Verfahren, die Windows Azure sicherer machen, beispielsweise die bei der Entwicklung von Windows Azure eingesetzten und weltweit anerkannten Prinzipien zur Integration der IT-Sicherheit in den Entwicklungsprozess (SDL, Security Development Lifecycle) von Microsoft, Maßnahmen zum Betrieb und zur Administration sowie physische Sicherheitsfeatures wie die Serverstandortwahl durch den Kunden, Zugang zum Rechenzentrum und redundante Stromversorgung.

Zum Schluss wird kurz das Thema Compliance behandelt, welches große Auswirkungen auf die IT-Organisation hat. Die Verantwortung für die Einhaltung gesetzlicher Regelungen, Vorschriften und Branchenanforderungen verbleibt grundsätzlich beim Windows Azure Kunden; Microsoft unterstützt sie aber dabei durch die Bereitstellung extensiver Sicherheitsmaßnahmen und eine stetig wachsende Zahl von Tools – denn darin liegt nicht nur Microsofts Schlüssel zum Erfolg, sondern auch der unserer Kunden.

August 2010

Inhalt

1 Einleitung

Windows Azure™ ist ein Betriebssystem für Cloud-Services, das als Dienstbereitstellungs-- und Service Management Umgebung für die Windows Azure-Plattform dient. Windows Azure bietet On-Demand Rechenkapazitäten, Storage sowie Skalierung und Management von Web Applikationen durch Microsoft® -Rechenzentren.

Mit Windows Azure stellt Microsoft Daten und Programme von und für Kunden bereit. Deshalb muss Windows Azure Sicherheitslösungen bieten, die weit über den üblichen Rahmen hinausgehen. Dieses Dokument erläutert die ganze Bandbreite von Kontroll- und Steuerungsmechanismen, die Ihnen als Kunde in Windows Azure zur Verfügung stehen.

1.1 Zielgruppe und thematische Eingrenzung

Dieses Whitepaper richtet sich vor allem an:

- Entwickler, die Interesse an der Anwendungsentwicklung für Windows Azure haben
- Technische Entscheider, die über Windows Azure als Plattform für neue oder bestehende Services nachdenken.

Schwerpunktthema dieses Whitepapers ist Windows Azure-als Plattform Komponente und „Betriebssystem für Online Services“. Es enthält keine detaillierten Erläuterungen zu den sonstigen Plattformkomponenten wie Microsoft SQL Azure, AppFabric oder Microsoft Codename „Dallas“.

Die Erläuterungen beziehen sich vornehmlich auf die Sicherheitsfeatures und -funktionalitäten von Windows Azure. Obwohl dieses Whitepaper auch allgemeine Informationen enthält, wird ein grundsätzliches Verständnis der Funktionsweise von Windows Azure beim Leser vorausgesetzt. Informationen über Aufbau und Funktion von Windows Azure erhalten sie in anderen Microsoft-Veröffentlichungen. Links zu weiterführenden Informationen finden sie im Abschnitt „Quellen und weiterführende Informationen“ am Ende dieses Dokuments.

Erläuterungen zu **fett** gedruckten Fachbegriffen finden Sie im Glossar, das sich ebenfalls am Ende des Dokuments befindet.

1.2 Allgemeines Sicherheitskonzept

Bevor wir tiefer auf die technischen Aspekte der Sicherheitsfeatures von Windows Azure eingehen, stellen wir in diesem Abschnitt kurz das zu Grunde liegende Sicherheitskonzept vor. Auch hier noch einmal der Hinweis: Der Leser sollte mit den Grundzügen von Windows Azure vertraut sein. Es geht in diesem Whitepaper primär um die sicherheitsrelevanten Aspekte.

1.2.1 Aus Kundensicht: Rechenleistung, Storage und Service Management

Windows Azure ist darauf ausgelegt, dass Kunden weite Teile ihrer IT-Infrastruktur auslagern können, die normalerweise zum Betrieb von Anwendungen erforderlich sind (Server, Betriebssysteme, Internet- und Datenbanksoftware etc.), sodass sich ihre Entwickler auf die Programmierung von Anwendungen konzentrieren können und sich nicht mehr um die Verwaltung der Infrastruktur kümmern müssen. Dieser Abschnitt vermittelt einen kurzen Überblick darüber, worauf ein typischer Kunde trifft, wenn er sich mit Windows Azure beschäftigt.

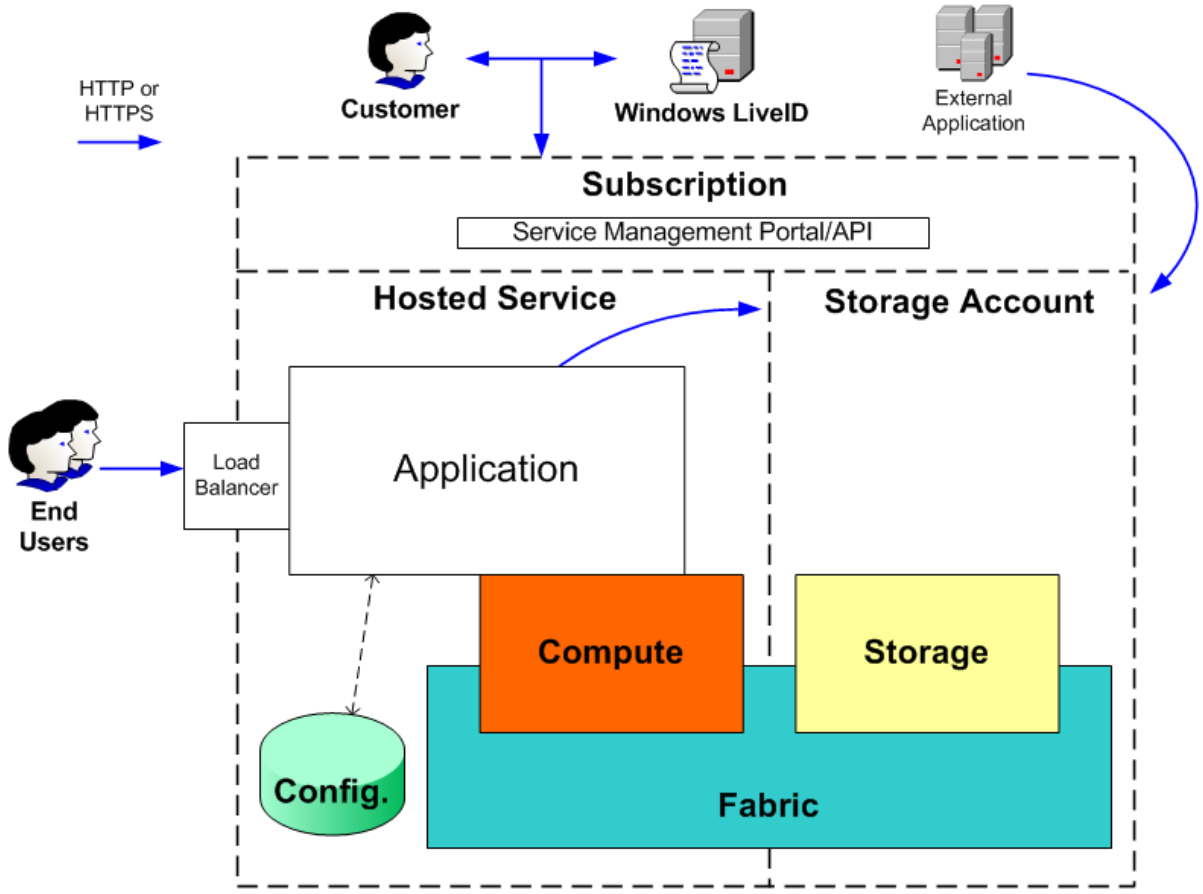

Abbildung 1: Vereinfachte Darstellung der wichtigsten Komponenten von Windows Azure

Wie in Abbildung 1 dargestellt, erfüllt Windows Azure zwei primäre Funktionen: Cloud-basierte Rechenleistung (Compute) und Datenspeicher (Storage). Auf dieser Grundlage können Sie als Kunde ihre Anwendung (Application) und die entsprechenden Konfigurationen aufbauen und verwalten. Anwendungen laufen auf Windows Azure als **Hosted Service**, der Zugriff auf den Storage Bereich erfolgt über einen **Storage Account**. Sie administrieren ihre Anwendung und den Storage über eine **Subscription (Abonnement).** Eine neue Subscription wird typischerweise durch Angabe einer Kreditkartennummer auf der Subscription-Website erstellt. Den Zugriff auf diese Subscription regelt anschließend der Windows Live ID Service (https://login.live.com). Windows Live ID ist einer der ältesten und bewährtesten Authentifizierungsdienste im Internet und dementsprechend ein strengstens getestetes und praxiserprobtes Zugangsportal zu Windows Azure.

Eine Subscription kann ohne einen Hosted Service oder Storage Account erstellt werden, kann später aber mehrere Hosted Services und mehrere Storage Accounts aufnehmen. Zu einem Hosted Service gehören ein oder mehrere Nutzer, zur Bereitstellung von Windows Azure mindestens eine oder mehrere **Rollen (Roles).** Eine Rolle verfügt über eine oder mehrere Instanzen. Storage Accounts enthalten Datenbanken mit BLOBs (Binary Large Objects), Tabellen und Queues. Das Windows Azure-Laufwerk ist eine spezielle Art von BLOB.

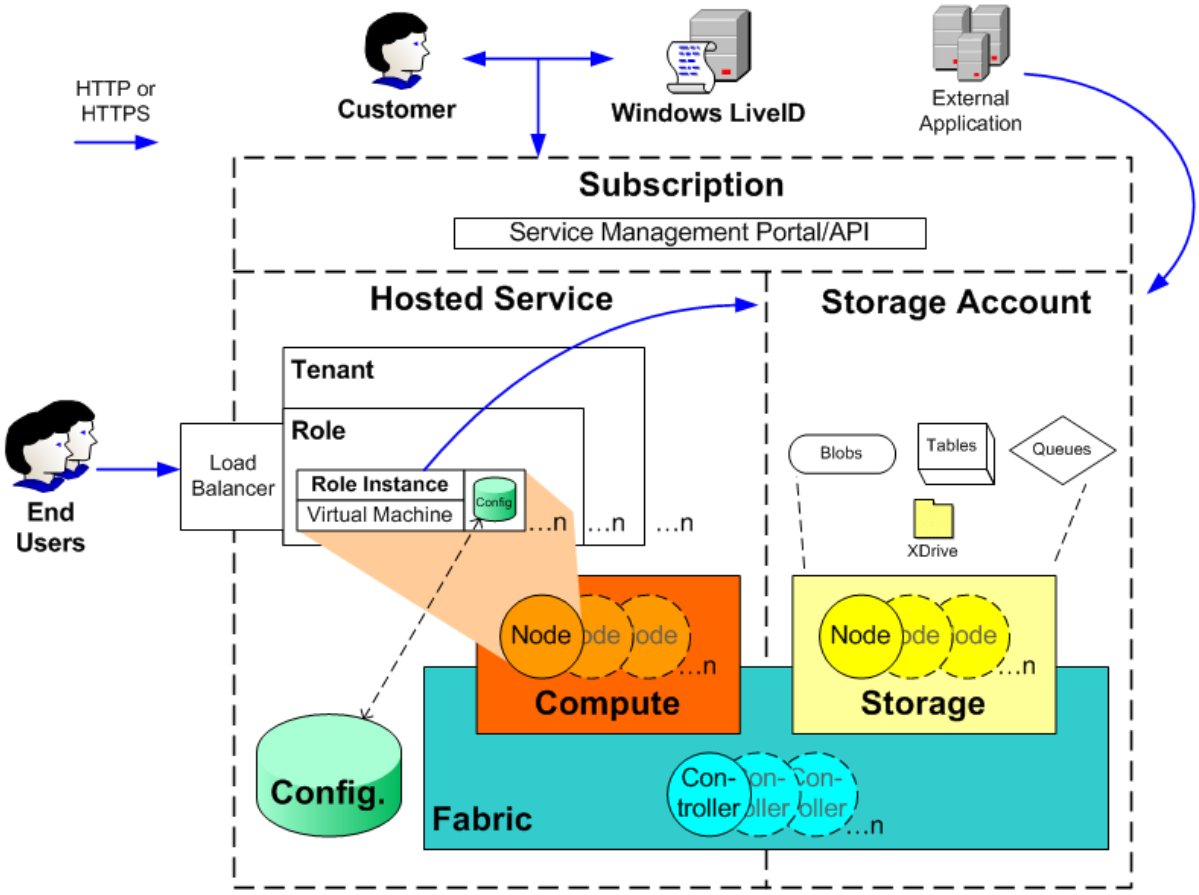

Abbildung 2: detailliertere Darstellung der Windows Azure-Komponenten und deren Beziehungen

Die Zugriffskontrolle auf die Hosted Services und Storage Accounts erfolgt über die Subscription. Die Authentifizierung mit der zugehörigen Live-ID gewährt volle Kontrolle auf alle zur Subscription gehörenden Hosted Services und Storage Accounts.

Sie können als Kunde selbst entwickelte Anwendungen entweder über das **Windows Azure Portal** hochladen und verwalten oder die Service Management API (SMAPI) nutzen. Der Zugriff auf das Windows Azure-Portal erfolgt über den Webbrowser, auf SMAPI per Befehlszeilentools oder über Visual Studio®.

Die SMAPI-Authentifizierung basiert auf einem benutzergenerierten öffentlich/privaten Schlüssel und einem selbst signierten Zertifikat, die beide über das Windows Azure-Portal ausgegeben werden. Das Zertifikat dient der Authentifizierung für den SMAPI Zugriff. SMAPI-Queues senden eine Anforderung an das Windows Azure Fabric, welches die gewünschte Anwendung initialisiert, zur Verfügung stellt und verwaltet.

Sie können als Kunde ihre Anwendungen mit dem gleichen Authentisierungsmechanismus über das Portal oder per SMAPI überwachen und verwalten.

Der Zugriff auf Windows Azure Storage erfolgt über einen Storage Account Key (SAK). Diese Schlüssel können über das Windows Azure Portal oder SMAPI geändert oder zurückgesetzt werden.[1]

Die Rechen- (compute) und Storageleistungen (storage) ergeben sich aus den grundlegenden Funktionseinheiten von Windows Azure. Abbildung 2 zeigt eine detaillierte Übersicht, aus der diese grundlegenden Einheiten und ihre Beziehungen zu den bisher beschriebenen Komponenten ersichtlich sind. Alle bisher beschriebenen Komponenten werden hier noch einmal zusammengefasst:

- Hosted Services beinhalten den Nutzungsdienst (Tenant), Rollen (Roles) und **Rolleninstanzen**
- Storage Accounts beinhalten BLOBs, Tabellen, Queues und Laufwerke.

Diese Begriffe werden im Glossar definiert. Weiterführende Informationen dazu können den allgemeinen Quellen zu Windows Azure entnommen werden. Sie werden hier kurz vorgestellt, um die nachfolgenden Erläuterungen zu den Sicherheitsfunktionalitäten von Windows Azure zu erleichtern.

Die jeweiligen Authentifizierungsmechanismen sind in der folgenden Tabelle zusammengefasst.

Nutzer	Objekte	Authentifizierungs-mechanismus
Kunden	Subscription (Rechenleistung und Storage)	Windows Live ID
Entwickler und Betreiber	Windows Azure-Webportal/API	Live-ID (Windows Azure Portal) oder selbst signiertes Zertifikat (SMAPI)
Rolleninstanzen	Storage	Storage Account Key (SAK)
Externe Anwendungen	Storage	Storage Account Key (SAK)
Externe Anwendungen	Anwendungen	Kundenspezifisch

Tabelle 1: Zusammenfassung der Windows Azure-Authentifizierungsmechanismen

[1] Es gibt weitere Zugriffskontrollmechanismen für Storage Accounts, die im Abschnitt 7 ausführlicher behandelt werden.

1.2.2 Aus Sicht von Microsoft: Windows Azure Fabric

Bisher wurden die Windows Azure-Komponenten beschrieben, die sie als Kunde verwalten können. Nun gehen wir auf das Windows Azure Fabric ein, auf das die Rechen- und Storageleistungen von Windows Azure basieren. Obwohl Sie als Kunde einzelne Aspekte dieser Fabric über definierte Management-Schnittstellen steuern können, liegt der Hauptzweck von Windows Azure gerade darin, dass die virtuelle Infrastruktur keines gesonderten Managements bedarf und für Sie als eine einzige konsistente, skalierbare Ressource erscheint. Sie als Entwickler müssen diese Infrastruktur nicht selbst verwalten, sondern Microsoft übernimmt dies für Sie. Dieser Abschnitt stellt einige der Basiskomponenten des Windows Azure Fabric vor, die von Microsoft verwaltet werden.

Basierend auf der von Ihnen festgelegten Anzahl von Rolleninstanzen generiert Windows Azure jeweils eine virtuelle Maschine (VM) pro Rolleninstanz. Die Rolle läuft dann auf diesen VMs. Die VMs laufen auf einem **Hypervisor** der speziell für den Einsatz in der Cloud ausgelegt ist (dem **Windows Azure Hypervisor**). Auf einer dieser VMs läuft ein extra gehärtetes (besonders gesichertes) Betriebssystem, das so genannte **Root-OS,** welches den **Fabric-Agent (FA)** bereitstellt. FAs werden wiederum zur Verwaltung von **Gastagenten (GA)** innerhalb der **Gastbetriebssysteme (Gast-OS)** auf den Kunden-VMs eingesetzt. FAs verwalten außerdem den Storagebereich. Windows Azure Hypervisor, Root-OS/FA und Kunden-VMs/-GAs sind die Bestandteile einer **Compute-Node** (eine Rechenleistungseinheit).

Das Management der FAs erfolgt durch einen **Fabric-Controller (FC)**, einer Software außerhalb der Compute-Node (**Cluster** werden von separaten FCs verwaltet). Wenn Sie als Kunde die **Konfigurationsdatei** ihrer Anwendung während der Laufzeit aktualisieren, kommuniziert der FC mit dem FA, der dann den GA kontaktiert und die Anwendung über die Konfigurationsänderung informiert. Bei einem Ausfall der Hardware sucht der FC automatisch nach verfügbarer Hardware und startet die VM dort neu.

2 Cloud Security Design

Windows Azure muss ein mindestens ebenso hohes Maß an *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* von Kundendaten liefern wie andere Application Hosting-Plattformen. Darüber hinaus muss für den Kunden und für Microsoft jederzeit transparent nachvollziehbar sein, wer Infrastruktur und Applikationen administriert. Aufbauend auf der bisherigen Beschreibung der Grundkomponenten und deren Beziehungen, legt dieser Abschnitt dar, wie Windows Azure jene klassischen Ausprägungen der Informationssicherheit sicherstellt.

2.1 Vertraulichkeit

Vertraulichkeit bedeutet “Schutz der Kundendaten vor unberechtigtem Zugriff“. Windows Azure nutzt dazu die folgenden Mechanismen:

- Identity und Accessmanagement – stellt sicher, dass ausschließlich Berechtigte, die sich als solche authentifiziert haben, auf die Daten zugreifen können.
- Isolation – minimiert die Interaktionen mit Daten durch logische oder physische Trennung von Datencontainern.
- Verschlüsselung – wird innerhalb von Windows Azure zum Schutz der Management Netze genutzt und wird optional für Kunden angeboten, die eine besonders hohe Datensicherheit benötigen.

Im Folgenden werden die einzelnen Datensicherungsmechanismen in Windows Azure ausführlich beschrieben.

2.1.1 Identity- und Accessmanagement

Selbst die stärksten Sicherheitskontrollen können nichts gegen Angreifer ausrichten, die sich unberechtigten Zugriff auf Zugangsdaten oder -schlüssel verschaffen. Deshalb gehört das Management von Zugangsdaten und -schlüsseln zu den entscheidenden Sicherheitskomponenten für Windows Azure.

Alle primären Identifizierungs- und Authentifizierungsmechanismen wurden bereits vorgestellt und sind in Tabelle 1 zusammengefasst. In diesem Abschnitt werden weitere Details zu entscheidenden Elementen wie APIs, Application Privilege Levels, Schlüsselverteilung und Zugangsdaten für vertrauenswürdige Subsysteme wie den Fabric-Controller behandelt.

2.1.1.1 SMAPI-Authentifizierung

Die Service Management API (SMAPI) bietet Webservices über das **Representational State Transfer (REST)** Protokoll und wird über Windows Azure-Tools den Entwicklern zur Verfügung gestellt. Das Protokoll läuft über SSL und authentifiziert sich mittels Zertifikat und privatem, vom Kunden generierten Schlüssel. Dieses Zertifikat greift nicht auf eine vertrauenswürdige Root Certificate Authority (CA) zurück, sondern ist selbst signiert und über das Windows Azure- Portal an die Subscription gekoppelt. Solange der Kunde also die alleinige Kontrolle über den privaten Schlüssel und die dazu gehörende Live-ID behält, bietet dieser Mechanismus ein Höchstmaß an Sicherheit, da ausschließlich vom Kunden autorisierte Personen auf die entsprechenden Services zugreifen können.

2.1.1.2 Least Privilege Software

Anwendungen mit „Least Privilege“, also mit den geringsten Rechten laufen zu lassen, gilt als „best practice“ Ansatz in der Informationssicherheit. Entsprechend diesem Prinzip erhalten Kunden keinen Administrationszugang zu ihren VMs. Die Software läuft in Windows Azure standardmäßig über ein Konto mit geringen Rechten (in künftigen Versionen können Kunden zwischen verschiedenen Rechtemodellen wählen).

Mögliche Angreifer müssten erst einmal die erforderlichen Rechte erlangen, um eine potenzielle Schwachstelle ausnutzen zu können. Diese Komplexität verringert die Erfolgswahrscheinlichkeit eines Angriffs signifikant. Darüber hinaus sind Kunden auch gegen Angriffe von Innentätern (z.B. demotivierte Mitarbeiter) geschützt.

2.1.1.3 Gegenseitige SSL-Authentifizierung bei der internen Steuerung

Jegliche Kommunikation zwischen internen Windows Azure-Komponenten ist geschützt. In den meisten Fällen sind die SSL-Zertifikate selbst signiert. Ausnahmen bilden der Fabric Controller und alle Zertifikate für Verbindungen, auf die von außerhalb des Windows Azure-Netzwerks zugegriffen werden kann (einschließlich Storage Services).

Fabric-Controller haben von einer Microsoft-CA ausgestellte Zertifikate, die auf eine vertrauenswürdige Root-CA zurückgreifen. Eine Verlängerung der öffentlichen FC-Schlüssel ist daher problemlos möglich. Darüber hinaus werden öffentliche FC-Schlüssel von Microsoft Developer Tools verwendet. Dadurch können neue Anwendungs-Images beim Hochladen automatisch mit einem öffentlichen FC-Zugangsschlüssel versehen werden, um größtmögliche Sicherheit zu gewährleisten.

2.1.1.4 Management von Zertifikaten und privaten Schlüsseln

Zertifikate und private Zugangsschlüssel für Entwickler und Administratoren werden zur Risikominimierung beim Ausstellen über einen anderen Mechanismus installiert als der Code, der sie benutzt. Zertifikate und private Schlüssel werden entweder über SMAPI oder das Windows Azure-Portal als **PKCS12-**(PFX-)Dateien über eine gesicherte SSL Verbindung übertragen. Diese PKCS12-Dateien können passwortgeschützt sein. Das Passwort muss dann aber in derselben Nachricht enthalten sein. SMAPI entfernt den Passwortschutz (falls erforderlich), verschlüsselt das gesamte PKCS12-Sytem mit einem öffentlichen SMAPI-Schlüssel und speichert diesen in einem versteckten Datenspeicher auf dem FC, zusammen mit einem kurzen Zertifikatsnamen und dem öffentlichen Schlüssel als Metadaten.

Die Konfigurationsdateien jeder Rolle innerhalb derselben Subscription geben unter anderem die Zertifikate an, die für die jeweilige Rolle zur Verfügung stehen muss. Wenn eine Rolle auf einer VM als Instanz läuft, fragt der FC das entsprechende Zertifikat ab, entschlüsselt den PKCS12-Blob, verschlüsselt diesen neu mit dem öffentlichen Transportschlüssel des FA und schickt ihn an den FA der entsprechenden Recheneinheit (node). Dieser FA schickt das Zertifikat dann an den GA auf der VM, auf der die Rolle als Instanz läuft. Der GA entschlüsselt es und installiert es im Zertifikatsspeicher des Betriebssystems mit einer Kennzeichnung, dass der private Schlüssel benutzt, aber nicht exportiert werden darf. Nach der Installation werden alle temporären Zertifikats- und Schlüsselkopien gelöscht. Sollte eine erneute Installation erforderlich sein, müssen die Zertifikate erneut vom FC zusammengestellt werden.

2.1.1.5 Nutzung von Hardwarezugangsdaten durch den FC

Zusätzlich zu den Anwendungsschlüsseln pflegt der FC einen weiteren Satz Zugangsdaten (Schlüssel und/oder Passwörter), die er zu seiner Authentifizierung gegenüber diversen Hardwaregeräten nutzt. Das System zum Transport, zur Aufrechterhaltung und zur Nutzung dieser Zugangsdaten ist so ausgelegt, dass Windows Azure-Entwickler, -Administratoren und -Back-up-Dienste bzw. Personal keinen Zugriff auf geheime Informationen benötigen. Zum FC-Setup und zur FC-Rekonfiguration wird eine Verschlüsselung auf Basis des öffentlichen Schlüssels der FC-Masteridentität eingesetzt, mit dem die Zugangsdaten für die Netzwerkhardware übertragen werden. Gleiches gilt für Remote Power Switches in den Serverracks, die für die zyklische Stromversorgung der Recheneinheiten und sonstiger Systeme eingesetzt werden. Der FC bewahrt diese geheimen Daten in seinem internen replizierten Datenspeicher (immer noch mit dem öffentlichen Schlüssel seiner Masteridentität verschlüsselt). Die Zugangsdaten werden nur abgerufen und entschlüsselt, wenn der FC sie benötigt.

2.1.1.6 Access Control im Windows Azure Storage

Wie bereits dargelegt, arbeitet der Windows Azure Storage mit einem einfachen Access Control Konzept. Jede Windows Azure-Subscription kann ein oder mehrere Storage Accounts erstellen. Jeder Storage Account hat einen geheimen Schlüssel, der zur Zugriffskontrolle auf alle Daten in diesem Storage Account verwendet wird. Dieses Verfahren unterstützt das typische Szenario, das einer Anwendung Storage zugewiesen wird und diese Anwendung volle Kontrolle über ihre Daten hat. Eine komplexere Zugriffskontrolle kann durch ein anwendungsspezifisches „Front End“ zum Storage hin erreicht werden. Die Anwendung erhält den Storage Key und kann selbst Remote Zugriffe authentifizieren und sogar einzelne Storage Anfragen autorisieren.

Zwei Mechanismen unterstützen generelle Access Control Szenarien. Ein Teil der Daten des Storage Accounts kann als *öffentlich lesbar* gekennzeichnet werden. Lese-Anfragen werden dann ohne Schlüsselsignatur zugelassen. Dieses Feature dient hauptsächlich dem Zugriff auf unkritische Daten wie Webseitenbilder.

Der andere Mechanismus heißt Shared Access Signature, SAS (*freigegebene Zugriffssignatur*). Dabei kann ein Prozess ein Anfrageformular (Query Template) generieren, welches er mit einem Storage Account Key (SAK) signiert. Die signierte URL kann dann an einen anderen Prozess weitergereicht werden, der weitere Angaben in das Formular einträgt und die Anfrage beim Storage Service durchführt. Obwohl diese Anfrage nun über einen „Dritten“ an den Storage Service gestellt wird, erfolgt die Authentifizierung immer noch über den SAK. Solche Auslagerungen können hinsichtlich Gültigkeitszeitraum und Berechtigungsumfang eingegrenzt werden.

Eine Shared Access Signatur kann sich auch auf eine *Container Level Access Policy* (Zugriffsrichtlinie auf Containerebene) beziehen, die einige Parameter in der URL austauscht (zum Beispiel Gültigkeitsdauer oder Berechtigungsumfang). Diese Parameter werden von der benannten Access Policy vorgegeben, die im Windows Azure Storage abgelegt ist. Da eine Container Level Access Policy jederzeit geändert oder verworfen werden kann, bietet sie mehr Flexibilität und Kontrolle über die zugelassenen Berechtigungen.

Ein Storage Account kann zwei Geheimschlüssel gleichzeitig haben (wobei beide Schlüssel jeweils vollen Datenzugriff gestatten). Dadurch können regelmäßig wechselnde SAKs ohne Dienstunterbrechung angeboten werden. Um einen Schlüssel zu ändern wird zunächst der neue Schlüssel im Storage Service angemeldet und autorisiert. Danach wird allen Anwendungen, die auf den Storage Service zugreifen, der neue Schlüssel mitgeteilt. Abschließend wird der alte Schlüssel entfernt. Die gültigen SAKs für einen Storage Account können entweder über SMAPI oder das Windows Azure Portal geändert werden.

2.1.2 Isolation

Neben der Authentifizierung des Datenzugriffs bietet die einfache Trennung von Daten anerkanntermaßen einen guten Schutz. Windows Azure ermöglicht die Datenisolation auf diversen Ebenen, wie nachfolgend beschrieben wird.

2.1.2.1 Isolation von Hypervisor, Root-OS und Gast-VMs

Eine wichtige Abgrenzung ist die Isolation der Root-VM von den Gast-VMs und die Abschirmung der Gast-VMs untereinander, die vom Hypervisor und dem Root-OS verwaltet werden. Die Paarung Hypervisor/Root-OS liefert die besten Resultate für die Isolation der Gast-VMs. Microsoft nutzt hier die jahrzehntelange Erfahrung mit Betriebssystemsicherheit und sein Know-how durch Microsoft Hyper-V.

2.1.2.2 Isolation des Fabric-Controllers

Da die Fabric-Controller die zentralen Dirigenten weiter Teile des Windows Azure Fabric sind, wurden hier hohe Schutzbarrieren gegen potenzielle Bedrohungen aufgebaut, insbesondere gegen möglicherweise veränderte/kompromittierte FAs von Kunden Applikationen.

Die Kommunikation von FC zu FA erfolgt nur in eine Richtung – der FA enthält lediglich einen SSL-Service, auf den der FC zugreift, und er antwortet auf Anfragen. Der FA kann selbst keine Verbindungen zum FC oder sonstigen wichtigen internen Systemen aufbauen. Der FC analysiert alle Antworten und behandelt sie zunächst als nicht vertrauenswürdig.

Darüber hinaus befinden sich die FCs und Geräte ohne SSL-Service auf separaten virtuellen LANs (VLANs), wodurch ein eventuell verändertes/kompromittiertes System nur eine sehr begrenzte Zahl solcher Authentifizierungsschnittstellen sehen kann.

2.1.2.3 Paketfilter

Der Hypervisor und das Root-OS stellen Netzwerkpaketfilter zur Verfügung, die dafür sorgen, dass die nicht vertrauenswürdigen VMs keinen vorgetäuschten Traffic generieren können (traffic spoofing), keinen Traffic empfangen können, der nicht an sie adressiert ist, keinen Traffic an geschützte Infrastrukturendpunkte weiterleiten können und auch keinen unsachgemäßen Broadcast Traffic senden oder empfangen können.

Storage Knoten (Storage nodes) laufen ausschließlich mit Code und Konfigurationen, die von Windows Azure stammen. Die Zugriffskontrolle erlaubt nur autorisierte Zugriffe von Kunden, Anwendungen und zu administrativen Zwecken.

Der Kundenzugriff auf die VMs wird durch Paketfilter der Load Balancer sowie im Root-OS begrenzt. Standardmäßig sind insbesondere Remote Debugging, Remote-Terminalservices oder Remotezugriff auf VM File Shares blockiert. Microsoft plant, dass Kunden zukünftig diese Protokolle optional explizit aktivieren können. Derzeit können Kunden bereits selbst wählen, ob Verbindungen aus dem Internet und von Rolleninstanzen innerhalb *derselben* Anwendung gestattet werden sollen.

Verbindungen zwischen Rolleninstanzen *verschiedener* Anwendungen werden als Internetverbindungen behandelt. Die Verbindungsregeln sind dabei kumulativ. Wenn die Rolleninstanzen A und B beispielsweise zu verschiedenen Anwendungen gehören, kann A nur dann eine Verbindung zu B herstellen, wenn A Verbindungen zum Internet aufbauen kann und B Verbindungen aus dem Internet zulässt.

Der Fabric-Controller übersetzt die Liste der Rollen in eine Liste der Rolleninstanzen und daraus in eine Liste von IP-Adressen. Diese Liste von IP-Adressen wird vom FA zur Programmierung der Paketfilter genutzt, damit die Anwendungskommunikation ausschließlich an diese IP-Adressen erfolgen kann. Rollen können dagegen auch an Internetadressen kommunizieren und Daten an jede beliebige andere Rolle senden, die vom Internet aus über ihre virtuellen IP-Adressen (**VIPs**) sichtbar ist.

2.1.2.4 Isolation virtueller LANs

VLANs werden zur Isolation der FCs und sonstiger Geräte genutzt. VLANs teilen ein Netzwerk so auf, dass keine Kommunikation zwischen VLANs möglich ist, außer über einen Router. Dadurch wird verhindert, dass ein eventuell kompromittiertes System Datenverkehr von außerhalb seines VLANs, außer gegenüber anderen Systemen in seinem VLAN, vortäuschen kann. Außerdem kann es außerhalb seines VLANs keinen Datenverkehr ausspionieren.

In jedem Cluster befinden sich drei VLANs:

- Das Haupt-VLAN – verbindet nicht vertrauenswürdige Kundensysteme.
- Das FC-VLAN – enthält vertrauenswürdige FCs und weitere Systeme.
- Das Device-VLAN – enthält vertrauenswürdige Netzwerk- und sonstige Infrastrukturgeräte.

Die Kommunikation zwischen FC-VLAN und Haupt-VLAN ist zulässig, kann aber ausschließlich vom FC-VLAN initiiert werden. Die Kommunikation vom Haupt-VLAN an das Device-VLAN ist blockiert. Dadurch wird sichergestellt, dass durch ein eventuell kompromittiertes Kundensystem keine Systeme über FC- oder Device-VLANs attackiert werden können.

2.1.2.5 Isolation der Kundenzugriffsplattform

Alle Systeme, die den Zugriff auf die Kundenumgebung verwalten (das Windows Azure-Portal, SMAPI etc.), sind in einer von Microsoft betriebenen Windows Azure-Anwendung isoliert. Dadurch ist die logische Trennung dieser Kundenzugriffsplattform und Anwendungen/Storage des Kunden sichergestellt.

2.1.3 Verschlüsselung

Sie können als Kunde Datenverschlüsselung im Storage und bei der Übertragung innerhalb von Windows Azure nutzen, um die Vertraulichkeit und die Integrität der Daten sicherzustellen. Wie bereits erwähnt, wird die interne Kommunikation durch eine SSL-Verschlüsselung geschützt. Mit dem Windows Azure Software Development Kit (SDK) können Sie die .NET-Kernbibliotheken erweitern und Entwicklern die Einbindung der .NET Cryptographic Service Providers (CSPs) in Windows Azure ermöglichen. Entwickler, die sich mit .NET-CSPs auskennen, können dann leicht Verschlüsselung, Hash-Algorithmen und Schlüssel-Management für gespeicherte oder übertragene Daten implementieren. Mittels der .NET-CSPs erhalten Windows Azure-Entwickler bequemen Zugriff auf z.B.:

- Anerkannte Verschlüsselungsalgorithmen wie AES, die sich seit vielen Jahren in der Praxis bewährt haben. Dadurch kann der klassische Fehler vermieden werden, sich an der Programmierung eigener Verschlüsselungsalgorithmen für Anwendungen zu versuchen.
- Eine große Anzahl kryptografischer Hash-Funktionalitäten, inklusive MD5 und SHA-2, zur Überprüfung der Datenrichtigkeit, zum Erstellen und Validieren digitaler Signaturen und zum Erstellen nicht identifizierbarer Merkmale (Token) für sensible Daten.
- Die RNGCryptoServiceProvider-Klasse zum Generieren einer hinreichend großen Anzahl von Zufallszahlen, um ein ausreichend hohes Entropie-Niveau für starke Kryptografie zu erzielen.
- Unkomplizierte Schlüssel-Management-Methoden, mit denen benutzerdefinierte Schlüssel im Windows Azure-Storage verwaltet werden können.

Links zu umfassenderen Darstellungen der Kryptografiefähigkeiten von Windows Azure finden Sie unter „Quellen und weiterführende Informationen“ am Ende des Dokuments.

2.1.4 Daten löschen

Die Vertraulichkeit von Kundendaten sollte auch über den eigentlichen Datenlebenszyklus hinaus bestehen. Das Windows Azure-Storage-Subsystem verhindert deshalb den Zugriff auf alle Daten, für die ein Löschbefehl durchgeführt wurde. Alle Speicheroperationen, einschließlich Löschen, sind auf sofortige Konsistenz ausgelegt. Ein erfolgreich abgesetzter Löschbefehl entfernt alle Verweise auf die entsprechenden Daten, sodass kein Zugriff über Storage-APIs mehr möglich ist. Alle Kopien der gelöschten Daten werden im Papierkorb zwischengespeichert. Genau wie bei herkömmlichen Computerfestplatten werden die physischen Bits überschrieben, sobald andere Daten auf dem entsprechenden Laufwerksblock gespeichert werden. Die Entsorgung physischer Speichermedien wird in Abschnitt 4.4.3 aufgegriffen.

2.2 Integrität

Kunden, die Rechenleistung und Storage an Windows Azure auslagern wollen, erwarten selbstverständlich auch, dass ihre Daten vor unberechtigten Änderungen geschützt sind. Das Cloud-Betriebssystem von Microsoft stellt dies auf vielfältige Weise sicher.

Der primäre Mechanismus zum Integritätsschutz von Kundendaten ist bereits im Design der Fabric-VM selbst begründet. Jede VM ist mit drei lokalen virtuellen Festplatten (VHDs) verbunden:

- Auf Laufwerk D: befindet sich eine von mehreren Versionen des Gastbetriebssystems, das laufend mit vom Kunden wählbaren relevanten Patches aktualisiert wird.
- Auf Laufwerk E: befindet sich ein vom FC erstelltes Image auf der Grundlage des vom Kunden bereitgestellten Softwarepakets.
- Auf Laufwerk C: befinden sich die Konfigurationseinstellungen, Paging-Dateien und sonstiger Storage.

Die virtuellen Laufwerke D: und E: befinden sich praktisch im Read-Only-Modus, weil ihre Access Control List (ACLs) keinen Schreibzugriff von Kundenseite zulassen. Da das Betriebssystem diese Read-Only-Laufwerke gegebenenfalls aktualisieren muss, sind sie als VHDs mit Delta-Dateien implementiert. Die ursprünglichen VHDs sind für alle Rolleninstanzen in einer Anwendung identisch. Das Delta-Laufwerk für Laufwerk D: wird jedes Mal ausgeworfen, wenn Windows Azure die VHD mit dem Betriebssystem patcht. Das Delta-Laufwerk für Laufwerk E: wird jedes Mal ausgeworfen, wenn die VHD mit einem neuen Anwendungsimage aktualisiert wird. So bleibt die Integrität des zu Grunde liegenden Betriebssystems und der Kundenanwendungen jederzeit strikt gewahrt.

Eine weitere primäre Integritätskontrolle ist die Konfigurationsdatei auf dem Read-Write-Laufwerk C:. Sie stellen als Kunde eine Konfigurationsdatei mit den Konnektivitätsanforderungen für alle Rollen in der Anwendung zur Verfügung. Der FC nimmt für jede Rolle den jeweils relevanten Befehlssatz aus dieser Konfigurationsdatei und legt ihn für jede Rolleninstanz auf Laufwerk C: ab. Wenn Sie die Konfigurationsdatei aktualisieren, während die Rolleninstanzen laufen, kontaktiert der Fabric-Controller (FC) – über den Fabric-Agent (FA) – den Gastagenten (GA) im Gastbetriebssystem der VM, und befiehlt ihm, die Konfigurationsdatei auf Laufwerk C: zu aktualisieren. Dann kann die Konfigurationsdatei von der Anwendung neu eingelesen werden.

Der Inhalt von Laufwerk C: wird dazu nicht verworfen, sodass Laufwerk C: der Kundenanwendung als ein stabiler Datenspeicher erscheint.[2] Die Konfigurationsdatei kann nur von autorisierten Kunden geändert werden, die über das Windows Azure-Portal oder SMAPI (wie bereits beschrieben) auf ihre Services zugreifen. Durch das zu Grunde liegende Design von Windows Azure ist die Integrität der Kundenkonfiguration folglich über die gesamte Anwendungslebensdauer permanent geschützt, aktuell und konsistent.

[2] Alle drei Laufwerke kehren in ihren Ursprungszustand zurück, falls die Rolleninstanz je auf ein anderes physisches Laufwerk transferiert wird. Zwecks Leistungsoptimierung sollten Kundenanwendungen deshalb Daten ausschließlich auf Laufwerk C: cachen.

Im Windows Azure Storage wird die Integrität über das bereits beschriebene Access Control Modell sichergestellt. Jeder Storage Account hat zwei Storage Account Keys (SAK), die zur Zugriffskontrolle auf alle Daten im Storage verwendet werden. Der Zugriff auf die SAK bietet folglich auch die volle Kontrolle über die entsprechenden Daten.

Die Integrität der eigentlichen Fabric wird sehr präzise gemanagt – vom Booten des Systems bis hin zum laufenden Betrieb. Wie bereits erläutert, ist das Root-OS, das auf VM-Hostingsystemen innerhalb des Fabric läuft, ein gehärtetes Betriebssystem. Nach dem Booten eines Systems startet dieses den Fabric-Agent (FA) und wartet auf Verbindungen und Befehle vom Fabric-Controller. Der FC nutzt hierfür die bereits beschriebene bidirektionale SSL Verbindung. Die Kommunikation des FC mit den FAs erfolgt unidirektional über „One-Way-Push“. Dadurch wird ein Angriff auf Komponenten, die höher in der Befehlskette stehen, schwierig weil keine Direktanfragen an diese Komponenten möglich sind. In Verbindung mit den vielen oben beschriebenen Sicherungsmechanismen sorgen diese Features dafür, dass das Fabric jederzeit in integerem, unverfälschtem Zustand ist.

2.3 Verfügbarkeit

Einer der Hauptvorteile von Cloud-Plattformen ist die hohe Verfügbarkeit durch extensive Redundanzen der virtuellen Systeme. Windows Azure bietet eine Vielzahl von Redundanz-Levels zur Gewährleistung der maximalen Verfügbarkeit von Kundendaten.

Daten werden in Windows Azure auf drei separate Systeme innerhalb des Fabric repliziert, um die Auswirkungen von Hardwaredefekten zu minimieren.

Sie können als Kunde mit einem zweiten Storage Account die Vorteile der geografisch verstreuten Windows Azure-Infrastruktur für „Fail-over“ Szenarien nutzen und so das Ausfallrisiko weiter senken. Sie können benutzerdefinierte Rollen zur Replikation und Synchronisation von Daten zwischen den Microsoft-Rechenzentren erstellen. Darüber hinaus können Sie auch mit benutzerdefinierten Rollen Backups auf externen Medien erstellen.

Die Gastagenten (GAs) auf jeder VM überwachen den Status der jeweiligen VM. Wenn der GA nicht antwortet, wird die VM vom FC neu gebootet. Künftig können sich Kunden optional auch für komplexere Monitoringprozesse entscheiden, die sich an benutzerdefinierten Continuity- und Recovery-Richtlinien orientieren. Im Falle eines Hardwaredefekts transferiert der FC die Rolleninstanz auf eine neue Hardware und programmiert die Netzwerkkonfiguration für die Rolleninstanz neu, um die volle Verfügbarkeit wiederherzustellen.

Jede VM besitzt ein Laufwerk D: mit vom Kunden frei wählbaren Versionen des Gastbetriebssystems. Der Kunde kann entweder manuell von einer Version des Gastbetriebssystems auf eine andere umstellen oder Microsoft seine Anwendungen umziehen lassen, wenn neue Versionen erscheinen. Dieses System maximiert die Verfügbarkeit während den normalen Wartungsarbeiten, bei minimalem Kundenaufwand.

FCs unterliegen ähnlichen Prinzipien der Hochverfügbarkeit durch Redundanzen und automatische Ausfallsicherung, wie sie auch für Kundendienste gelten. Das Ergebnis ist eine permanente Verfügbarkeit der FCs. Während eines Upgrades der Windows Azure-Plattform oder einer Kundensoftware verwenden FCs eine logische Partition, eine sogenannte *Update-Domain,* um Teile einer bestimmten Rolleninstanz zu einem vordefinierten Zeitpunkt zu ändern, während die übrigen Instanzen weiterhin Anfragen abarbeiten. Durch die Spezifikation von *Fault-Domains* erfahren FCs außerdem von potenziellen Hardware- und Netzwerkfehlern. Windows Azure stellt für alle Dienste mit mehr als einer Rolleninstanz sicher, dass diese Instanzen auf mehreren Update- und Fault-Domains bereitgestellt werden (sofern nicht vom Kunden anders festgelegt). Dadurch ist die volle Verfügbarkeit des Dienstes auch während der Installation von Updates und Teilausfällen der Netzwerkhardware sichergestellt.

2.4 Rechenschaft und Transparenz

Da Cloud-Computing-Plattformen de facto eine Auslagerung von Rechenleistung darstellen, sollten Sie als Kunde regelmäßig den *Nachweis* eines sicheren Betriebs erhalten. Windows Azure gewährleistet diese Transparenz durch mehrere Monitoring Levels, Logging und Reportingfunktionen. Insbesondere der **Monitoring-Agent (MA)** sammelt Monitoring- und Diagnosedaten aus vielen Quellen, einschließlich FC und Root-OS und schreibt diese in Logdateien. Am Ende schiebt er eine aufbereitete Version dieser Daten in einen vorkonfigurierten Windows Azure-Storage Account. Der **Monitoring Data Analysis Service (MDS)** ist ein zusätzlicher, eigenständiger Dienst, der diverse Log-Dateien aus Monitoring und Diagnose liest, diese zusammenfasst und aufbereitet sowie die Ergebnisse in ein integriertes Log schreibt.

3 Sicherheit während des Development Lifecycles

Microsoft setzt anerkannte und bewährte Tools und Techniken ein, um die Sicherheit von Windows Azure bereits in der Konzeptions- und Entwicklungsphase sowie bei der Implementierung des Dienstes selbst zu gewährleisten.

Die Microsoft-Richtlinien „Security Development Lifecycle (SDL)“ sind in vollem Umfang in die Entwicklung von Windows Azure eingeflossen und haben internationalen Vorbildcharakter für die Softwaresicherheit (weitere Informationen zu SDL finden Sie unter „Quellen und weiterführende Informationen“).

Dazu zählt insbesondere, dass Microsoft alle Stellen einer genauesten Prüfung unterzieht, an denen eine vertrauenswürdige Komponente Daten von einer weniger vertrauenswürdigen Komponente analysiert. Das gilt beispielsweise:

- Wenn der Windows Azure Hypervisor und das Root-OS Anfragen zur Ein-/-Ausgabe auf Laufwerken oder Netzwerken von kundengesteuerten VMs verarbeiten.
- Wenn Storage Accounts Anfragen verarbeiten, die von kundengesteuerten Systemen über das Netzwerk kommen.

- Wenn der Fabric-Controller (FC) Kundenkonfigurationsdaten analysiert, die über SMAPI eingegangen sind.

Neben sorgfältiger Konzeption und Implementierung werden diese Komponenten auch mit hoch entwickelten Programmiersprachen wie C# entwickelt, wodurch die Wahrscheinlichkeit einer Speichermanipulationen deutlich gesenkt wird. Darüber hinaus erfolgen umfangreiche Tests aller Schnittstellen, bevor das Fabric produktiv geschaltet wird. Microsoft wendet diese Methode standardmäßig auch auf alle Upgrades und Änderungen von Code an, welcher externe Anfragen verarbeitet.

Die SDL-Richtlinien von Microsoft werden allen Windows Azure-Kunden ans Herz gelegt, da die Sicherheit der Anwendungen auf Windows Azure auch stark von den Entwicklungsprozessen beim Kunden abhängig ist. Auf der Microsoft Webseite ist der Leitfaden *Security Best Practices For Developing Windows Azure Applications* abrufbar (siehe „Quellen und weiterführende Informationen“).

Selbst wenn sowohl Microsoft als auch der Kunde SDL umsetzen, bleibt noch eine minimale Restwahrscheinlichkeit, dass die Software zwischen der Entwicklung und der Bereitstellung auf Windows Azure kompromittiert wird. Deshalb liefert der Kunde die Daten für seine Anwendungen direkt über SMAPI, das – neben anderen Sicherungsmechanismen – Zertifikatsauthentifizierung und HTTPS-geschützte Kanäle für die Codeübertragung einsetzt.

4 Windows Azure im Betrieb

Die möglicherweise wichtigsten Sicherheitsfaktoren der Plattform sind die Menschen und Prozesse, die für den Betrieb von Windows Azure sorgen. Dieser Abschnitt befasst sich deshalb mit der Infrastruktur der Microsoft-Rechenzentren, die zur Verbesserung und Wahrung von Sicherheit, Kontinuität und Datenschutz beitragen.

4.1 Microsoft-Betriebspersonal

Windows Azure-Entwickler und -Administratoren sind mit entsprechenden Rechten ausgestattet, um die ihnen zugewiesenen Aufgaben bei Betrieb und Entwicklung zu erfüllen. Es wurde bereits dargelegt, dass Microsoft Kombinationen verschiedener präventiver, zustandsbasierter und reaktiver Kontrollmechanismen einsetzt. Dazu zählen auch die folgenden Mechanismen zum Schutz gegen unberechtigte Aktivitäten von Entwicklern und/oder Administratoren:

- Strikte Zugriffskontrollen auf sensible Daten.
- Kombinationen verschiedener Kontrollmaßnahmen zur leichteren Entdeckung böswilliger Aktivitäten.
- Monitoring, Protokollierung und Reporting auf diversen Ebenen.

Darüber hinaus überprüft Microsoft die Mitarbeiter im Rechenzentrum und grenzt deren Zugriff auf Anwendungen, Systeme und Netzwerkinfrastruktur ein.

Microsoft-Mitarbeiter dürfen nur nach Kundenaufforderung auf Kundenkonten oder sensible Daten zugreifen und müssen dabei strenge Formalien einhalten.

4.2 Meldungen sicherheitsrelevanter Vorfälle

Schwachstellen und Sicherheitslücken können dem Microsoft Security Response Center gemeldet werden. (http://www.microsoft.com/security/msrc/default.aspx oder per E-Mail an secure@microsoft.com). Microsoft geht allen Meldungen nach, die über diese Kanäle eingereicht werden.

4.3 Netzwerk Administration

Eine kritische Komponente von Windows Azure ist sicherlich die Netzwerkinfrastruktur, mit der alle Komponenten untereinander verbunden sind. Dieser Abschnitt erläutert einige der Sicherheitsmaßnahmen, die auf dieser Ebene getroffen werden.

Es wurde bereits dargelegt, dass das interne Windows Azure-Netzwerk durch starke Filter gegen Datenverkehr von anderen Netzwerken abgeschottet ist. Dadurch wird für Hochgeschwindigkeit im internen Netzwerk-Traffic gesorgt, der generell nur geringe Sicherheitsrisiken aufweist.

Die Konfiguration und Verwaltung von Netzwerkgeräten, wie Switches, Router und Load-Balancer, erfolgt ausschließlich durch autorisiertes Microsoft-Personal und normalerweise nur bei größeren Änderungen (z.B. bei einer Rekonfiguration des Rechenzentrums). Die Virtualisierung durch das Windows Azure Fabric macht solche Änderungen für Kunden praktisch unsichtbar.

Darüber hinaus wird jede Hardwarekomponente, die nicht die Anforderungen an Kommunikationssicherheit (wie z.B. SSL) erfüllt, über ein separates LAN verwaltet, das gegenüber Systemen mit Internetzugang oder Kundenzugang abgeschottet ist.

4.3.1 Remote Administration von Fabric-Controllern

Fabric-Controller verfügen über eine Schnittstelle für den Remotezugriff (RPC-fähige API), die Befehle von SMAPI und von Windows Azure-Administratoren verarbeitet. Entscheidungen auf Richtlinienebene werden von SMAPI auf der Anwendungsebene umgesetzt und erlauben nur Anfragen zu kundenspezifischen Ressourcen, wenn die ID des Kunden authentifiziert wurde. Die FCs treffen dagegen als zentrale Managementstelle engmaschigere Zugriffskontrollentscheidungen.

Verbindungen zu FCs erfolgen grundsätzlich über SSL, die Authentifizierung des Clients dementsprechend über ein Client-Zertifikat. Anhand des Zertifikats wird dann entschieden, ob die erforderliche Zugriffsberechtigung für die gewünschte Anfrage vorliegt.

4.4 Physische Sicherheit

Ein System kann nicht sicherer sein als die physische Plattform, auf der es läuft. Windows Azure läuft gemeinsam mit anderen Microsoft-Online-Diensten in geografisch verteilten Microsoft-Rechenzentren. Alle Standorte sind auf einen 24 x7 Betrieb ausgelegt und weisen diverse Sicherheitsvorkehrungen auf, um Strom- und Netzwerkausfälle sowie das Eindringen von Unbefugten zu verhindern. Die Rechenzentren erfüllen alle Branchenstandards zur physischen Sicherheit und Zuverlässigkeit und werden von Microsoft-Mitarbeiter verwaltet und überwacht. Sie sind außerdem auf energieeffizienten Einsatz ausgelegt. Einzelheiten zur physischen Sicherheit von Windows Azure sind in den folgenden Abschnitten beschrieben.

4.4.1 Zutritt zu Gebäuden

Microsoft setzt branchenübliche Zutrittsmechanismen und Sicherheitstechniken zum Schutz der physischen Infrastruktur und der Rechenzentren für Windows Azure ein. Lediglich einer sehr kleinen Gruppe von Mitarbeitern wird der Zutritt gestattet. Die Zugangscodes werden regelmäßig geändert. Die Zutrittsberechtigungen für Rechenzentren und die Erteilung von Zutrittsberechtigungen werden von Microsoft-Mitarbeitern anhand strenger lokaler Sicherheitspraktiken für Rechenzentren überwacht.

4.4.2 Redundante Stromversorgung und Ausfallsicherheit

Alle Rechenzentren verfügen über mindestens zwei getrennte Stromversorgungen und besitzen eigene Stromgeneratoren für den Weiterbetrieb bei Ausfall des öffentlichen Stromnetzes. Die Klimatisierung erfolgt eigenständig und hält die Umgebungsbedingungen so lange konstant aufrecht, wie das Rechenzentrum und die darin enthaltenen Systeme online sind.

Während eines Stromausfalls oder sonstigen Störung sind die physisch erreichbaren Zugänge darauf ausgelegt zu schließen. Bei Bränden oder sonstigen lebensbedrohlichen Situationen können die Gebäude über Notausgänge zügig verlassen werden.

4.4.3 Entsorgung von Speichermedien

Am Ende ihres Lebenszyklus werden alle Systeme nach strengen Richtlinien zum Umgang mit Daten, Speichermedien und Hardware durch Microsoft-Mitarbeiter entsorgt.

5 Compliance

Die Bedeutung von Compliance hat durch die starke Zunahme weltweit gültiger Normen, wie ISO 27001, Safe Harbor und vieler weiterer massiv zugenommen. Die Nichterfüllung dieser Standards kann in vielen Fällen dramatische Auswirkungen auf Unternehmen zur Folge haben. Schlimmstenfalls drohen empfindliche Geldstrafen und/oder schwere Imageverluste.

Alle vorgenannten Bedrohungsszenarien können sich auch auf die Compliance auswirken. Darüber hinaus gibt es weitere Bedrohungen, wie beispielsweise mangelnde Umsetzung anerkannter Praktiken, unvollständige Compliance-Dokumentation gegenüber Auditoren, oder fehlende Unterstützung für die elektronische Beweissicherung.

Microsoft stellt alle erforderlichen Informationen zur Verfügung, damit Sie als Kunde entscheiden können, ob im Kontext von Windows Azure die Einhaltung aller Gesetze und Vorschriften möglich ist, denen sie unterliegen. Darüber hinaus erhalten Sie auch die erforderlichen Tools zum Compliance-Nachweis, falls dieser möglich ist. Im Folgenden sind einige Punkte erläutert, mit denen Windows Azure Kunden beim Thema Compliance unterstützt werden.

5.1 Serverstandortwahl durch den Kunden

Eine der größten Herausforderungen beim Einsatz von Windows Azure ist, das Gleichgewicht zwischen den Compliance-Anforderungen und den großen wirtschaftlichen Vorteilen von Cloud-Diensten zu finden: Denn die Daten und die Infrastruktur des Kunden werden auf mehrere Systeme und (weltweite) Standorte verteilt, sodass sie auch unterschiedlicher Rechtsprechung unterliegen. Windows Azure bietet eine sehr einfache Lösung: Kunden können frei wählen, wo ihre Daten gespeichert werden. Die Daten werden ausschließlich in Microsoft-Rechenzentren in der Region gespeichert, die der Kunde über das Windows Azure-Portal ausgewählt hat. Durch die freie Serverstandortwahl können Compliance-Risiken sehr einfach minimiert werden.

5.2 Compliance-Kontrollmechanismen

In diesem Dokument wurden viele der Kontrollmechanismen in Windows Azure vorgestellt, die eine praxisnahe Compliance-Erfüllung bieten. Hier noch einmal eine tabellarische Aufstellung der wichtigsten Compliance relevanten Sicherheitsfeatures:

Thema	Relevante Abschnitte	Zusammenfassung
Zugriffskontrolle	1.2	Windows Azure bietet diverse Zugriffskontrollen zum Schutz gegen unberechtigten Datenzugriff von Administratoren oder Endbenutzern.
Verschlüsselung	2.1.3	Die Verschlüsselungseinstellungen können für den Storagebereich und die Übertragung von Daten in Windows Azure festgelegt werden, um die gewünschte Vertraulichkeit und Integrität der Daten zu erzielen.
Verfügbarkeit	2.3, 4.4	Kunden können benutzerdefinierte Rollen für Back-ups erstellen. Die physische Infrastruktur von Windows Azure ist über verschiedene Standorte verteilt.
Datenschutz	2.1.4	Im Windows Azure Storage werden vom Kunden gelöschte Daten restlos und nachhaltig vernichtet.

5.3 Zertifizierung nach ISO 27001

Unabhängige Zertifizierungen sind international ein bewährtes Instrument für den Nachweis, dass Kundendaten bestens geschützt sind. Windows Azure arbeitet in der Infrastruktur der Microsoft Global Foundation Services (GFS), die zum Teil nach ISO27001 zertifiziert ist. Die ISO-Norm 27001 ist einer der wichtigsten anerkannten internationalen Sicherheitsstandards in der Informations-technologie. Darüber hinaus sind derzeit noch weitere Branchenzertifizierungen für Windows Azure in Vorbereitung.

Neben der ISO27001-Zertifizierung gehört die Microsoft Corporation auch zu den Unterzeichnern von Safe Harbor und hat sich zur Einhaltung aller Vorgaben durch das Safe Harbor Framework verpflichtet.

Obwohl die Verantwortung für die Erfüllung von gesetzlichen Regelungen, Vorschriften und Branchenanforderungen bei Windows Azure-Kunden verbleibt, unterstützt Microsoft seine Kunden mit den oben beschriebenen Features bei der Compliance-Erfüllung.

6 Quellen und weiterführende Informationen

In den folgenden Quellen finden Sie allgemeinere Informationen zu Windows Azure und verwandten Microsoft-Services sowie zu einzelnen Punkten, auf die in diesem Text Bezug genommen wird:

- Windows Azure-Homepage – allgemeine Informationen und Links zu weiteren Quellen über Windows Azure; http://www.microsoft.com/windowsazure/
- Windows Azure Developer Center – Hauptinformationsquelle für Entwickler; http://msdn.microsoft.com/en-us/windowsazure/default.aspx
- Security Best Practices For Developing Windows Azure Applications – http://download.microsoft.com/download/7/3/E/73E4EE93-559F-4D0F-A6FC-7FEC5F1542D1/SecurityBestPracticesWindowsAzureApps.docx
- Crypto Services and Data Security in Windows Azure – http://msdn.microsoft.com/en-us/magazine/ee291586.aspx
- Microsoft's Security Development Lifecycle – SDL ist das Microsoft-Qualitätssicherungsverfahren für Sicherheit, das bei der Entwicklung von Windows Azure angewendet wird; www.microsoft.com/security/sdl/
- Microsoft's Global Foundation Services Security – verantwortlich für die vertrauenswürdige und verfügbare Online-Betriebsumgebung, die Windows Azure zu Grunde liegt; http://www.globalfoundationservices.com/security/

- Microsoft GFS' ISO 27001 Zertifizierung – http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/CertificateClient-Directory-Search-Results/?pg=1&licencenumber=IS+533913&searchkey=companyXeqXMicrosoft
- Microsoft Security Response Center – Microsoft-Sicherheitslücken, einschließlich Schwachstellen bei Windows Azure, können gemeldet werden an: http://www.microsoft.com/security/msrc/default.aspx oder per E-Mail an secure@microsoft.com

7 Glossar

Glossarbegriff	Definition
Anwendung (Application)	Eine Sammlung von VM-Rolleninstanzen, die zusammengenommen einen Hosted Service liefern.
Cluster	Eine Sammlung von Hardware-Modulen, die von einem einzelnen Fabric-Controller gesteuert werden.
Endbenutzer	Endbenutzer sind alle Personen, die auf Dienste zugreifen, die über den Windows Azure Fabric bereitgestellt werden. Das können beispielsweise Mitarbeiter oder Kunden des Kunden sein (laut Definition „Kunde"). Sie greifen typischerweise über das Internet auf diese Dienste zu (außer es handelt sich bei den Endbenutzern um andere Windows Azure-Kunden, wodurch die Anfragen aus dem Windows Azure Fabric kommen könnten, aber trotzdem wie Internetanfragen behandelt werden). Endbenutzer werden von der Windows Azure-Infrastruktur und/oder der benutzerdefinierten Kundenkonfiguration grundsätzlich als nicht vertrauenswürdig eingestuft, sodass die Infrastruktur Schutzmechanismen gegen Endbenutzer beinhaltet und unseren Kunden ermöglicht, ihre Dienste davor zu schützen.
FA (Fabric-Agent)	Eine Komponente des Root-OS, die einen SSL-Port öffnet, der eingehende Verbindungen und Anfragen vom Fabric-Controller akzeptiert sowie lokale Konfigurationseinstellungen auf dem System vornimmt, inklusive Erstellen und Löschen von VMs. Der FA aktualisiert sich selbst sowie die lokal gespeicherten Betriebssystem Images.

Glossarbegriff	Definition
FC (Fabric-Controller)	Die Software zur Ausführung von Management und Einrichtung der physischen Hardware, Zuweisung von Speicherplatz, CPU-Ressourcen, RAM und VMs an Kunden, für die Bereitstellung von Anwendungs- und Betriebssystem-Images und für die Programmierung der Paketfilter zur Steuerung der Konnektivität innerhalb des Fabric. Der FC ist auch am Systeminitialisierungsprozess beteiligt, indem er die Betriebssystemimages für den Remote Netzwerk Bootvorgang über das Intel Framework Preboot eXecution Environment (PXE) zustellt.
Hosted Service	Ein kundenspezifischer, Cloud basierter Dienst, der von Microsoft-Kunden auf Windows Azure betrieben wird.
GA (Gastagent)	Ein von Windows Azure bereitgestellter Agent innerhalb der Gast-VM, der bestimmte Dienste wie z.B. den Health Index der Rollen und die Installation von Zertifikaten und privaten Zugangsschlüsseln vornimmt. Dieser Agent kommuniziert über eine nicht öffentliche Verbindung zum FA in der Root-Partition mit der Außenwelt. Obwohl GAs von Windows Azure bereitgestellt werden, laufen sie innerhalb des Sicherheitskontextes einer Anwendung und gelten deshalb innerhalb des Sicherheitsmodells von Windows Azure als Anwendungscode.
Gastbetriebssystem	Ein auf Kompatibilität mit Windows Azure getestetes Betriebssystem, das für den Kunden auf einer VM läuft. Alle Gastbetriebssysteme sind so konzipiert, dass sie normalerweise mit einer bestimmten Version von Windows Server kompatibel sind.
Hypervisor	Die Softwarekomponente, die für die Isolation des gesamten Kundencodes sorgt, der auf Windows Azure läuft. Er läuft direkt auf der Hardware und teilt ein System (einen „node“) in eine variable Anzahl von VMs. Zusammen mit dem Root-OS setzt er Barrieren für die Außenkommunikation und teilt Ressourcen ein.
Load-Balancer	Eine Netzwerkkomponente, die eingehenden Internet-Traffic an Windows Azure annimmt und an eine geeignete IP-Adresse und einen Port innerhalb des Fabric weiterleitet. Der Load-Balancer weist die Verbindungen so zu, dass die Rechenlast gleichmäßig auf mehreren verschiedenen Servern oder VMs verteilt wird, die eine eingehende Anfrage bearbeiten können. Die Routing-Tabellen des Load-Balancers müssen aktualisiert werden, wenn VMs erstellt, gelöscht oder von einer Hardwarekomponente auf eine andere transferiert werden.

Glossarbegriff	Definition
Konfigurationsdatei	Der Kunde stellt eine einzige Konfigurationsdatei bereit, in der die Verbindungsanforderungen aller Rollen in der Anwendung festgelegt sind. Der FC nimmt für jede Rolle den jeweils relevanten Befehlssatz aus dieser Konfigurationsdatei und legt ihn für jede Rolleninstanz/VM auf Laufwerk C: ab. Wenn der Kunde die Konfigurationsdatei aktualisiert, während die Rolleninstanzen laufen, weist der Fabric alle VMs an, ihre Konfigurationsdateien zu aktualisieren, und befiehlt dann der Kundenanwendung, ihre Konfigurationsdatei neu einzulesen.
Kunde	Kunde bezeichnet in diesem Dokument denjenigen, der von Microsoft Windows Azure Ressourcen kauft, um darauf Anwendungen laufen zu lassen. Dazu gehören auch interne Microsoft-Gruppen, die ihre Anwendungen über Windows Azure bereitstellen.
MA (Monitoring-Agent)	Ein Agent, der an vielen Orten läuft, inklusive FC und Root-OS, Monitoring- und Diagnosedaten sammelt und diese in Logdateien schreibt. Am Ende schiebt er eine aufbereitete Version dieser Daten in einen vorkonfigurierten Windows Azure-Storage Account.
MDS (Monitoring Data Analysis Service)	Ein eigenständiger Dienst, der diverse Monitoring- und Diagnose Logdateien liest, die Daten zusammenfasst/aufbereitet und die Ergebnisse anschließend in ein integriertes Log schreibt.
Paketfilter	Ein Mechanismus für Netzwerkrichtlinien, der Einschränkungen der IP-Konnektivität innerhalb des Windows Azure Fabric durchsetzt, und der von der Root-Partition eines Nodes implementiert wird.
PKCS12	Einer der Public-Key Cryptography Standards (PKCS), die von den RSA Laboratories herausgegeben werden. Dieser Standard definiert ein Dateiformat zur Speicherung von privaten X.509 Schlüsseln zusammen mit den dazugehörigen öffentlichen Schlüsselzertifikaten, gesichert durch einen passwortgeschützten symmetrischen Schlüssel.
Recheneinheit, -system (compute node)	Eine Recheneinheit setzt sich aus Hypervisor, Root-OS/FA und Kunden-VMs/-GAs zusammen.
REST (Representational State Transfer)	Ein RPC-Protokoll (Remotezugriff), das über das Netzwerkprotokoll SOAP läuft und für viele Interaktionen innerhalb des Windows Azure Fabric und mit Windows Azure-Kundenentwicklungsumgebungen genutzt wird.

Glossarbegriff	Definition
Rolle	Ein Prozess innerhalb einer Anwendung, der aus zwei oder mehr identischen Rolleninstanzen besteht, die über diverse Systeme verteilt sind, um Skalierbarkeit und Fehlertoleranzen zu erzielen. Jeder Hosted Service hat mindestens eine Rolle, die meisten haben zwei oder drei. Komplexe Dienste können eine Vielzahl Rollen haben. Der Begriff „Rolle“ bezeichnet auch gelegentlich die Gesamtheit von Code und Konfigurationseinstellungen, die das Rollenverhalten festlegen und zur Erstellung von Rolleninstanzen auf single-node Systemen verwendet werden.
Rolleninstanz	Ein Prozess in einer VM, der eine einzelne Instanz als Teil einer Rolle innerhalb einer Anwendung erstellt. Um Skalierbarkeit und Verfügbarkeit zu erzielen, laufen normalerweise mehrere Instanzen einer Rolle gleichzeitig. Falls ein bestimmter Hosted Service zu einem gegebenen Zeitpunkt nicht laufen sollte, gäbe es keine Rolleninstanzen für dessen Rollen. Der Begriff „Rolleninstanz“ bezeichnet auch gelegentlich die gesamte VM-Instanz, die eine einzelne Rolleninstanz bereitstellt. Rolleninstanzen entsprechen normalerweise 1:1 den internen/NAT`d Windows Azure-IP-Adressen.
Root-OS	Ein gehärtetes (besonders gesichertes) Betriebssystem, das in der ersten VM auf der Recheneinheit läuft und als Host für den Fabric-Agent agiert. Dieses Basisbetriebssystem enthält nur die zum Betrieb von VMs erforderlichen Komponenten. Dies steigert die Leistung und bietet zeitgleich eine geringere Angriffsfläche gegenüber Angreifern.
SMAPI (Service Management API)	Ein Hosted Service, der Windows Azure-Kunden die Schnittstellen-API für Code bereitstellt. Windows Azure-Entwickler greifen mit dem REST-Protokoll auf SMAPI zu, das mit SSL-Authentifizierung durch ein über das Windows Azure-Webportal generiertes Zertifikat arbeitet.
Subscription	Ein Windows Azure-Kundenkonto, über das die Abrechnung für Hosted Services und Storage Accounts abgewickelt wird.
VHD (Virtual Hard Disk)	Eine Imagedatei, in der Betriebssysteme, Kundensoftware und temporärer Speicherstand in einem einheitlichen Format gespeichert werden, also eine Spiegelung einer einzelnen Computerfestplatte.
VIP (Virtual IP Address)	Eine von außen sichtbare IP-Adresse, über die Kunden mit Hosted Services auf Windows Azure kommunizieren. Die VIP wird von Load-Balancern implementiert, die den Traffic bestimmten Endpunkten zuweisen (hauptsächlich Rollen).

Glossarbegriff	Definition
VM (Virtual Machine)	Eine softwareseitige Emulation eines Computers, die in einem virtuellen Speichermanager läuft (VMM oder Hypervisor) und sich wie ein physischer Computer verhält.
Windows Azure Hypervisor	(Siehe Hypervisor.)
Windows Azure-Portal	Eine Website, über die Kunden ihre Hosted Services und Storage Accounts verwalten.
Windows Azure-Laufwerk	Das Windows Azure-Laufwerk ist ein dauerhaftes NTFS-Laufwerk für Windows Azure-VM-Instanzen. Genau genommen ist das Windows Azure Laufwerk ein BLOB (Binary Large Object), der alle Schreibvorgänge im BLOB des Storage Accounts konserviert. Wenn die VM mit einem eingebundenen (mounted) Laufwerk ausfällt, existiert das Laufwerk immer noch als BLOB und kann ohne Datenverlust an anderer Stelle erneut eingebunden (gemountet) werden. Die Windows Azure-Laufwerke werden normalerweise wie ein NTFS-Image auf einer physischen Festplatte formatiert. Windows Azure-VMs können diese als Festplatten mounten und dann wie auf normale Dateisysteme darauf zugreifen. Der Windows Azure-Code cacht die Daten aus dem Windows Azure-Laufwerk auf seiner lokalen Festplatte, um deutliche Leistungsverluste beim Lesen zu umgehen. Während BLOBs, Tabellen und Queues der Storage Accounts auf das Öffnen und Aktualisieren durch mehrere unabhängige VMs ausgelegt sind, kann der Lese/Schreib-Zugriff auf das Windows Azure-Laufwerk nur durch eine VM erfolgen. Snapshots des Laufwerks können allerdings im Nur-Lese-Modus von einer unbegrenzten Zahl von VMs eingebunden werden, wodurch die Aktualisierung verteilter, replizierter Prozesse erschwert wird. Windows Azure-Laufwerke stellen eine Kompatibilität für Anwendungen sicher, die einen nativen NTFS Zugriff benötigen.