Projektskizze (Kurzfasung)

# Sichere und hochverfügbare Vertrauenskontexte für Mixed-Cloud-Szenarien (Secure and highly-available Trust contexts for mixed CLOUD scenarios, SATCLOUD)



Univention GmbH
Mary-Somerville-Straße 1
28359 Bremen


Deutsches Forschungszentrum für Künstliche Intelligenz GmbH
Sichere Kognitive Systeme (SKS)
Enrique-Schmidt-Straße
28359 Bremen

# Inhaltsverzeichnis

# Zusammenfassung

Cloud-Computing ist in der Zukunft ein zentraler Bestandteil von IT-Infrastruktur in Organisationen. Typischerweise werden dabei jedoch nicht alle Bestandteile der IT-Infrastruktur in die Cloud migriert, sondern weiterhin vorhandene Bestandteile lokaler IT-Infrastruktur mit Cloud-Lösungen integriert (sog. „Mixed Cloud“).

Ziel des Projekts ist die Erweiterung der Technologie zur Umsetzung von administrativen Konzepten („Domain“, „Vertrauenskontext“), mit denen einfache Administrierbarkeit in der Organisations-IT realisiert wird, zur Verwendung in Mixed Cloud-Umgebungen. Das wird es vielen Organisationen ermöglichen, Cloud-basierte Dienste wirtschaftlich, sicher und kontrolliert nutzen zu können.

Dazu soll eine Sprache entwickelt und implementiert werden, in der verschiedene Vertrauensstufen, differenzierte Sichten und Konfliktlösungsstrategien bei Multimaster-Replikation für die Cloud formuliert werden können. Die Projektergebnisse werden als Open Source-Software bereitgestellt, wodurch hohe Transparenz und gute Akzeptanz für die breite und erfolgreiche Vermarktung der Lösung über unterschiedliche Cloud-Anbieter, Systemintegratoren und Softwarehersteller erreicht werden soll.

# 1. Zielsetzung

## Problemstellung

Zur konzeptionellen und praktischen Vereinfachung der Administration von heterogenen IT-Infrastrukturen sowie der darauf zugreifenden Identities und deren Berechtigungen wird heute typischerweise mit Vertrauenskontexten gearbeitet. Ein Vertrauenskontext beinhaltet verschiedene Objekte wie Rechner, Benutzer, Richtlinien oder Dateien sowie deren Beziehungen zueinander. Diese Objekte und ihre Beziehungen können an einer Stelle zentral administriert werden. Die so definierten Regeln gelten dann für alle Systeme, die zu dem entsprechenden Vertrauenskontext gehören. Durch die Verwendung von Vertrauenskontexten müssen Administratoren somit Konfigurations- und Sicherheitsrichtlinien oder etwa Zugriffsberechtigungen nicht für jedes System einer Infrastruktur separat festlegen, sondern können dies an einer Stelle zentral für alle Systeme der Infrastruktur tun. Dies reduziert Komplexität und Arbeitsaufwand bei der Administration und erhöht so die Sicherheit.

Zukünftig werden Organisationen jedoch vermehrt Anwendungen und Infrastrukturbestandteile verwenden, die sie nicht selbst in ihrer lokalen Infrastruktur betreiben, sondern die als eine Form des Cloud-Computings von Dienstleistern in deren Rechenzentrum oder im Rechenzentrum eines Dritten als individuelle oder standardisierte Dienstleistung bereit gestellt werden.

Die heute verfügbaren Cloud-Angebote stellen jedoch weitgehend von der weiterhin vorhandenen lokalen IT-Infrastruktur der Anwenderorganisation und auch voneinander isolierte Anwendungen und Infrastrukturbestandteile dar, die sich entweder gar nicht oder nur mit hohem individuellen Aufwand miteinander oder mit der lokalen IT-Infrastruktur integrieren lassen. Diese Beschränkung stellt Administratoren vor viele zusätzliche Aufgaben, im Ergebnis müssen sie ein sehr viel höheres Komplexitätsniveau bewältigen.

## Lösungsanforderungen und Anwendungsbeispiel

Erforderlich ist deswegen die Erweiterung des Konstruktes „Vertrauenskontext“ auf so genannte „Mixed-Cloud“-Umgebungen. Dieser Begriff bezeichnet IT-Infrastrukturen, die sich aus Komponenten zusammensetzen, die zum Teil klassisch lokal beim Anwender betrieben werden und sich zum anderen Teil bei einem oder mehreren unterschiedlichen Anbietern von Cloud-basierten Lösungen befinden. In dem Moment, in dem Organisationen die selbst betriebenen und die bei verschiedenen Anbietern befindlichen Dienste und Anwendungen in „ihren“ Vertrauenskontext zusammenfügen können, finden sie zu den gewohnten Paradigmen zurück und können Cloud-basierte Dienste ähnlich einfach wie lokale Dienste heute

administrieren. Das wird es vielen Organisationen ermöglichen, Cloud-basierte Dienste wirtschaftlich nutzen zu können.

Mixed-Cloud-Umgebungen stellen jedoch zusätzliche, neue Anforderungen an Vertrauenskontexte. Da sich die den Kontext nutzenden Infrastrukturbestandteile bei unterschiedlichen Anbietern (mit unterschiedlichen Sicherheitsniveaus) befinden und weil für unterschiedliche Anwendungen in der Regel unterschiedliche Sicherheitsanforderungen gelten, muss es Administratoren auf einfache, transparente Weise ermöglicht werden, zu bestimmen, welche Aspekte eines Vertrauenskontextes für einzelne oder Gruppen von Anwendungen und Infrastrukturbestandteilen gelten, bzw. von diesen überhaupt gesehen werden können. So kann es beispielsweise gewünscht sein, nur einer kleinen Anzahl von Anwendern den Zugriff auf eine bei einem bestimmten Cloud-Anbieter betriebene Anwendung zu geben. Ferner kann gewollt sein, dass dieser Cloud-Anbieter nur die für die Verwendung der Applikation benötigten Identity-Informationen der Benutzer sieht, die diese Anwendung auch benutzen dürfen. Alle anderen Identities der betreffenden Organisation sind dann aus Sicht der Cloud-Anwendung nicht existent.

Die Ausdehnung von Vertrauenskontexten über mehrere Rechenzentren unterschiedlicher Cloud-Anbieter stellt darüber hinaus neue Anforderungen an Verfügbarkeit der den Vertrauenskontext steuernden Informationen. Dazu gehört beispielsweise die Notwendigkeit, administrative Informationen für einen Bestandteil der Infrastruktur ändern zu können, wenn ein anderer gerade nicht verfügbar ist. So ist es sehr wünschenswert auch dann noch Mailkonten anlegen zu können, wenn die lokal betriebene IT-Infrastruktur teilweise oder vollständig nicht verfügbar sein sollte.

Um eine solche Hochverfügbarkeit der Vertrauenskontexte zu garantieren, ist eine beiderseitige selektive Replikation mit Multimaster-Fähigkeit und Möglichkeit zur verteilten Administration erforderlich. Diese muss darüber hinaus so realisiert werden, dass auch nur die für einen bestimmten Dienst benötigten Objekteigenschaften in den Zugriffsbereich des Infrastruktur-Betreibers repliziert und dort vorgehalten werden, wo der entsprechende Dienst auch betrieben wird.

## Ziele des Projekts

Das Projekt hat das Ziel, die erhöhten Anforderungen an Vertrauenskontexte für die erfolgreiche Verwendung in Mixed-Cloud-Szenarien systematisch zu definieren, und die so genannte „SATCLOUD-Sprache“ zu entwickeln, in der verschiedene Vertrauensstufen, differenzierte Sichten und Konfliktlösungsstrategien für die Multimaster-Replikation formuliert und umgesetzt werden können. Diese Sprache soll prototypisch als eine Erweiterung von Univention Corporate Server implementiert werden. Die Projektergebnisse werden als Open Source-Software bereitgestellt. Damit wird für die zu entwickelnde Technologie ein hohes Maß an Herstellerunabhängigkeit realisiert, was ein hohes Maß an Vertrauen von Softwareherstellern, Systemintegratoren sowie von Cloud-Anbietern in diese Technologie und damit ein hohes Maß an Adaption ermöglicht.

Im Enterprise-Bereich haben sich Zugriffspolitiken des Role-Based Access Control (RBAC) zur Spezifikation der Autorisierung von Diensten etabliert. Die Zuordnung von Berechtigungen und Benutzern zu Rollen erlaubt in der Regel eine redundanzfreiere Formalisierung einer Sicherheitspolitik als sie in herkömmlichen auf Access Control Lists (ACLs) basierenden Mechanismen (in denen die Rollen quasi “ausmultipliziert” werden) möglich wäre. Für die Spezifikation der Vertrauenskontexte sollen daher rollenbasierte Autorisierungsverfahren zum Einsatz kommen, die über LDAP-Directories abgewickelt werden.

## Allgemeines wirtschaftliches Interesse

Cloud-Computing beschreibt einen aktuellen Trend mit großem Marktpotenzial, der sich erst in den nächsten Jahren voll entwickeln wird. Im Kern geht es beim Cloud-Computing um einen Paradigmenwechsel bei Betrieb, Angebot und Kauf IT-bezogener Produkte und Dienstleistungen: Diese werden von IT-Anwendern nicht mehr als einzelne Komponenten im Rahmen von IT-Investitionen beschafft, sondern bedarfsabhängig als fertige Lösungen eingekauft. Das Investitions- und Betriebsrisiko geht dabei auf den Cloud-Anbieter über, der die Anwendungen in einem Rechenzentrum für seine Kunden betreibt und quasi verbrauchsabhängig abrechnet. IT wird dadurch für Anwender zu einer wirtschaftlich viel besser

beherrschbaren Größe, die -wie beispielsweise der Bezug von Strom- keine besonderen Investitionen mehr erfordert.

Insbesondere für kleine und mittelgroße Unternehmen bietet Cloud-Computing das Potenzial, Professionalität, Sicherheit, Skalierbarkeit und Verfügbarkeit der von ihnen genutzten IT-Komponenten in einem hohen Maß zu steigern. Denn diese Unternehmen können heute nur mit hohen Kraftanstrengungen eine professionelle und modernen Standards genügende IT-Infrastruktur betreiben. Die Verlagerung von IT-Bereitstellung und -Betrieb zu Dienstleistern, welche die selben Dienste in Rechenzentren für sehr viele Kunden übernehmen, wird deswegen grundsätzlich zu einer deutlichen Verbesserung dieser Situation führen.

Doch auch für Softwareanbieter und IT-Dienstleister bietet Cloud-Computing hohe wirtschaftliche Potenziale: Beide können fertige IT-Lösungen in viel besser beherrschbaren Umgebungen betreiben und durch die kontinuierliche, verbrauchsabhängige Abrechnung einen fortlaufenden Einnahmestrom erzeugen.

Faktisch gibt es bei der Adaption von Cloud-Angeboten durch professionelle IT-Anwender heute jedoch wichtige technologische Hindernisse, von denen wichtige durch dieses Projekt aufgegriffen und beseitigt werden sollen. Denn damit IT anwendende Organisationen Cloud-Angebote auch tatsächlich adaptieren und wirtschaftlich nutzen können, müssen verschiedene Voraussetzungen erfüllt sein, dazu gehört neben vielen andernorts beschriebenen Bedingungen insbesondere, dass

1. die heute für viele Organisationen schon hohe Komplexität von Betrieb und Administration von IT durch die Integration von Cloud-Angeboten zumindest nicht weiter erhöht wird (Ziel und Produktversprechen vieler Cloud-Angebote ist sogar die Reduktion von Komplexität),
2. Cloud-Angebote von verschiedenen Anbietern eingekauft, die entsprechenden Angebote miteinander kombiniert und Angebote unterschiedlicher Anbieter miteinander ausgetauscht werden können und
3. IT-Anwender die Kontrolle darüber behalten, welche Informationen sie an einen Cloud-Anbieter weitergeben.

Hinsichtlich dieser Punkte realisiert dieses Projekt entscheidende Verbesserungen und schließt somit die Lücke zwischen privater IT-Infrastruktur und Cloud-Diensten: Anwender können damit die in Zukunft aus lokaler IT und weit verbreiteten, zugekauften Cloud-Diensten bestehenden IT-Umgebungen wie bisher zentral und mit Hilfe eines einheitlichen Vertrauenskontextes verwalten, aber dabei kontrollieren, welche Informationen und Sichten welchem Anbieter zur Verfügung gestellt werden. Gleichzeitig werden Abhängigkeiten von der Verfügbarkeit einzelner Cloud-Anbieter, lokaler IT oder bestimmter Netzwerkverbindungen auf andere Komponenten minimiert, so dass im Falle des Ausfalls einer Komponente immer nur die betreffende Komponente für den Anwender nicht verfügbar ist.

# 3. Projektbeschreibung

## Sichten auf Domains in der Mixed Cloud

Die für Organisationen realistischen Szenarien im Bereich IaaS sind Mixed Cloud-Szenarien, d.h. ein Teil der IT-Infrastruktur (in der Regel der sensiblere) bleibt lokal im Unternehmen, während ein anderer Teil in die Cloud ausgelagert wird. Für die Benutzung und Administration der IT-Infrastruktur soll diese Unterteilung jedoch weitgehend transparent sein, so dass Anwender in der Regel gar nicht merken, ob sie lokal oder in der Cloud arbeiten. Für die Sicherheitspolitik des Unternehmens ist die Unterscheidung in lokale IT-Infrastruktur und Cloud jedoch sehr bedeutsam: sensible Bereiche sollen vermutlich nicht in die Cloud ausgelagert werden. Zudem wird das Vertrauen des Unternehmens in verschiedene Cloud-Anbieter variieren, und bestimmte Daten dürfen laut Bundesdatenschutzgesetz nur im Inland gespeichert werden - es gibt bereits Cloud-Anbieter, die einen bestimmten Standort in der Cloud garantieren. Dies führt zur Notwendigkeit verschiedener Vertrauens- oder Sicherheitsstufen, mit denen die verschiedenen Cloud-Anbieter belegt werden.

In diesem Projekt soll daher die so genannte “SATCLOUD-Sprache” entwickelt werden, die es zunächst ermöglicht, die bekannten Replikations-Mechanismen für Domains mit Vertrauenskontexten zu formulieren. Diese Sprache soll dann erweitert werden um Sichten für die Mixed Cloud. Zentrale Herausforderung sind

hier der dezentrale Charakter der Cloud, die damit verbundenen Vertrauensstufen und das Management von Sicherheitsgrenzen. Mittels Sichten kann festgelegt werden, welche Server welche Identity- und Authentifizierungsdaten sehen und replizieren dürfen. Typischerweise wird ein Server in der Cloud nur eine eingeschränkte Sicht auf die LDAP-Daten haben dürfen. Eine Sicht, die Vertrauensstufen in der Cloud folgt, kann dabei quer zu Subdomains oder organisatorischen Einheiten liegen, die ja die baumartige organisatorische Gliederung abbilden. Sie kann z.B. mehrere Subdomain-Teilbäume umfassen und andere ausschließen, ebenso wie einzelne Attribute und Objektklassen. Einfache Szenarien sollen einfach konfigurierbar sein; dafür sollen sowohl das Design der SATCLOUD-Sprache als auch eine grafische Schnittstelle (GUI) sorgen.

Der Sprachumfang der SATCLOUD-Sprache soll gängige in der Praxis auftretende Konfigurationsaufgaben umfassen, wie z.B. Sicherheitsstufen für Dateisystem, Print-Server, Groupware bzw. Desktop-Virtualisierung. Die Sprache soll auf Konfigurationsmöglichkeiten für den Fall vorsehen, das ein Server von Cloud-Anbieter A nach Cloud-Anbieter B migriert wird. Dabei müssen die Vertrauensstufen und Sichten ja ggf. geändert werden. Sichten für die Cloud gehen mit dieser dynamischen Sichtweise damit deutlich über die bekannte fractional replication hinaus.

### Multimaster-Fähigkeit in der Cloud

Identity-Management und Vertrauenskontexte sind zentrale Steuerungsinformationen der IT-Infrastruktur eines Unternehmens, die hochverfügbar sein müssen, um stets handlungsfähig zu sein. Die oben beschriebene Multimaster-Fähigkeit von Directory-Servern stellt die (auch schreibende) Administrierbarkeit von Teilen eines IT-Systems auch beim Ausfall einzelner Server und Netzwerkverbindungen sicher. Dies ist natürlich in der Cloud von gesteigerter Bedeutung. Die von Active Directory verwendete Konfliktlösungsstrategie (jüngere Einträge haben höhere Priorität) ist jedoch in der Cloud nicht immer angemessen. Ein Unternehmen wird für die Konfliktlösung auch die verschiedenen Vertrauensstufen der Cloud mit einbeziehen wollen, so dass Directory-Server in der Cloud bei der Konfliktlösung niedrigere Priorität bekommen. Die in diesem Projekt entwickelte Sprache für Sichten auf Domains soll verschiedene solche Konfliktlösungsstrategien explizit ermöglichen, und die Konfliktlösung soll transparent sein.

Eine weitere Herausforderung ist die Integration der Änderungen, die über verschiedene Sichten gemacht wurden, zu einer konsistenten Identity-Datenbank. Es ist bekannt, dass asynchrone Replikation bereits ohne Sichten nur lose Konsistenz erreichen kann, d.h. eine global konsistente Datenbank entsteht durch die Replikation erst nach und nach. Durch Sichten kann dieses Problem noch verschärft werden. Wir nehmen deshalb an, dass mindestens ein Master-Directory Server die vollständige Sicht auf alle Identity-Daten hat; solche Server sind dann verantwortlich für die Sicherung globaler Konsistenz. Diese geschieht in den meisten Fällen automatisch anhand der in der SATCLOUD-Sprache ausgedrückten Politiken; in wenigen Fällen wird eine manuelle Konfliktlösung nötig sein.

Auf diese Weise entsteht die SATCLOUD-Sprache, die globale Politiken für Server in Mixed Cloud-Umgebungen ausdrücken und gleichzeitig flexibel auf den dynamischen Charakter der Cloud eingehen kann.

Microsoft Active Directory-Domain-Controller können als Master mit einbezogen werden, indem sie jeweils lokal mit einem UCS-Domain-Controller vernetzt sind, der dann -sozusagen als Brückenkopf- die Verbindung zum restlichen Netz der Domain-Controller herstellt. Der Brückenkopf verhält sich zum AD-Controller wie ein solcher, so dass lokal die Konfliktlösungsstrategie von Microsoft greift, global aber die hier beschriebene.

## 7. Anteil der Antragsteller

Nicht zuletzt wegen der räumlichen Nähe der beiden Projektpartner (die Firmensitze von DFKI-SKS und Univention befinden sich in nur fünf Minuten Fußweg voneinander) soll das Projekt in einer sehr engen Zusammenarbeit zwischen beiden Projektpartner durchgeführt werden. Das bedeutet, dass alle Arbeitspakete von beiden Projektpartnern gemeinsam bearbeitet werden, wenngleich auch mit unterschiedlichen Schwerpunkten. So wird ein nachhaltiger Austausch zwischen der wissenschaftlichen Expertise des DFKI und der umfangreichen Erfahrung bei der professionellen Entwicklung und Pflege von Softwareprodukten von Univention sichergestellt. Außerdem führt dieses Vorgehen dazu, dass das im Projekt entwickelte

Know-How nach Projektabschluss für Univention verwertbar ist und in Form marktreifer Produkte umgesetzt werden kann.

## DFKI

Der Forschungsbereich Sichere Kognitive Systeme des DFKI Bremen hat eine langjährige Erfahrung im Bereich formaler Entwicklungsmethoden, Änderungsmanagement und IT-Sicherheit. Dies sind auch die zentralen Themen, mit denen sich das DFKI in diesem Projekt engagiert. Am DFKI werden beispielsweise in laufenden BMBF- bzw. DFG-Projekten die Integration heterogener Prozesse und die damit verbundenen Anpassungsmechanismen, die Verifikation und Reparatur von Sicherheitsprotokollen sowie die Konzepte für formale Sicherheitsmodelle untersucht.

## Univention

Univention bringt in das Projekt jahrelange Erfahrung bei der verantwortlichen Pflege und Weiterentwicklung von Open Source-Produkten für den Betrieb und die Verwaltung von IT-Infrastrukturprodukten sowie bei der erfolgreichen Entwicklung neuer Produkte in diesem Bereich ein. Dazu gehören umfangreiche Kenntnisse und Erfahrung bei der professionellen Entwicklung, Dokumentation und Qualitätssicherung von Software, ein sehr breites Wissen über die für den Projektgegenstand relevanten Open Source-Softwarepakete sowie wichtiger proprietärer Softwaresysteme und 10 Jahre Markterfahrung mit einem umfassenden Netzwerk von Technologiepartnern, Systemintegratoren und Endkunden.