5.3 Das vRealize-Automation-Rollenkonzept

Nachdem wir in diesem Kapitel bereits die wichtigsten logischen Konzepte von vRealize Automation erläutert haben, werfen wir an dieser Stelle einen Blick auf die Sicherheit, d.h. auf das in vRealize Automation vorhandene Rollenkonzept. Einige Rollen, wie der Tenant-Administrator, der IaaS-Administrator oder der Fabric-Administrator, wurden bereits erwähnt, sollen jedoch hier der Vollständigkeit halber noch mal aufgelistet werden.

In vRealize Automation werden systemweite Rollen, Tenant-Rollen und Business-Group-Rollen unterschieden. Systemweite Rollen umfassen den Systemadministrator, den Infrastructure-Administrator und den Fabric-Administrator. Tabelle 5–1 zeigt hierfür die genauen Berechtigungen.

Rolle	Berechtigungen
Systemadministrator	■ Installation von vCloud Automation Center ■ Anlegen und Konfigurieren von Tenants ■ Monitoring der Systemlogs ■ Einrichten des Brandings und Anbindung des E-Mail-Servers
IaaS-Administrator	■ Verwalten von Endpunkten und Credentials ■ Erzeugen von Fabric Groups ■ Konfiguration der Proxy-Agenten ■ Administrieren der Cloud Service Accounts
Fabric-Administrator	■ Verwalten von physischen Maschinen und Compute Resources in einer Fabric Group ■ Verwalten von Reservations und Reservation Policies ■ Definition von Build Profiles und Machine Prefixes ■ Anlegen von Cost Profiles

Tab. 5–1 *Systemweite Rollen*

Bei den Tenant-Rollen existieren der Tenant-Administrator, der Service-Architekt und der Approval-Administrator. Tabelle 5–2 zeigt die Berechtigungen dieser Rollen.

Rolle	Berechtigungen
Tenant-Administrator	■ Verwalten des Tenants ■ Verwalten von Benutzern und Gruppen ■ Administration des Service Catalog ■ Definieren von Genehmigungsrichtlinien ■ Zuweisen von Berechtigungen auf den Service Catalog ■ Tenant Branding ■ Erstellen und Verwalten von globalen Blueprints
Service-Architekt	■ Anlegen und Veröffentlichen von Service Blueprints mit dem Advanced Service Designer
Approval-Administrator	■ Definieren von Genehmigungsrichtlinien

Tab. 5–2 *Tenant-Rollen*

Die Business-Group-Rollen bestehen aus dem Business Group Manager, dem Support User, dem Business User und dem Approver (siehe Tab. 5–3).

Rolle	Berechtigungen
Business Group Manager	■ Anlegen und Veröffentlichen von Blueprints ■ Verwalten von Berechtigungen und vorhandenen Objekten im Service Catalog ■ Monitoring des Ressourcenverbrauchs
Support User	■ Anlegen von Maschinen für andere Personen
Business User	■ Anfordern und Verwalten von Ressourcen
Approver	■ Genehmigung von Anforderungen

Tab. 5–3 *Business-Group-Rollen*

5.4 Tenant-Design

Wie beim Einrichten von komplexer Software üblich, sollte vor der eigentlichen Implementierung das Design der Lösung konzipiert werden. Insbesondere das Tenant-Design ist von besonderem Interesse. Aus diesem Grund soll in diesem Abschnitt erläutert werden, welche Gestaltungspielräume sich beim Einrichten von Tenants ergeben.

Ein Tenant stellt eine Organisationseinheit in einer vRealize-Automation-Center-Umgebung dar. Als solche kann er auf eine Business Unit in einer Firma oder einen Mandanten eines Cloud-Serviceproviders abgebildet werden. Jeder Tenant hat seine eigene Konfiguration, teilt sich aber Einstellungen mit anderen Mandanten.

Beim Design ist es möglich, sich zwischen einem *Single-Tenant Deployment* und einem *Multi-Tenant Deployment* zu entscheiden. Der folgende Abschnitt stellt beide Alternativen vor.

5.4.1 Vergleich zwischen Single-Tenant und Multi-Tenant Deployments

Systemweite Konfiguration, wie z.B. Notifications und Branding, werden immer im Default Tenant definiert und gelten standardmäßig für alle Tenants.

Die Infrastrukturkonfiguration dagegen kann in einem beliebigen Tenant definiert werden und wird dann über Tenant-Grenzen hinweg geteilt. Infrastrukturressourcen (zum Beispiel Cloud oder Virtual Compute Resources) werden zu Fabric Groups zusammengefasst. Diese werden von Fabric-Administratoren verwaltet. Die Ressourcen innerhalb der Fabric Groups sind dann in Tenants mittels Reservierungen an Business Groups zuzuweisen.

5.4.2 Single-Tenant-Konfiguration

In der Single-Tenant-Konfiguration erfolgt die Konfiguration im Standard-Tenant. Tenant-Administratoren verwalten User und Gruppen, das Branding, Notifications, Business Policies und den Service Catalog. Alle User benutzen die gleiche URL zum Einloggen (`https://<vrealize-automation-appliance.domain.name>/vcac/org`). Dabei erscheint das User-Interface aber je nach Berechtigung unterschiedlich.

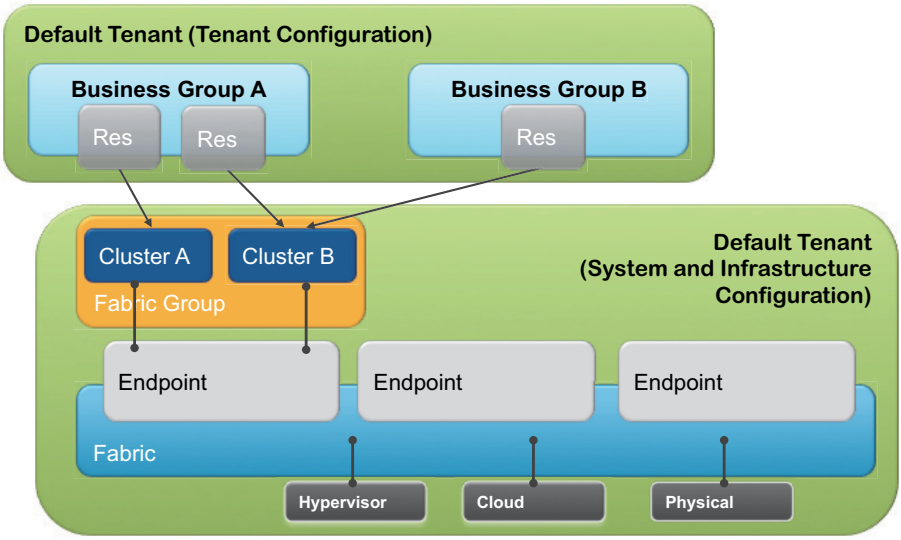

Abb. 5–22 *Single-Tenant-Design*

Technisch ist das Single-Tenant-Design (siehe Abb. 5–22) am einfachsten abzubilden und eignet sich besonders für kleinere und mittlere Unternehmen mit einem zentralen Administrationsteam. Im Unternehmenseinsatz ist daher dieser Ansatz am häufigsten anzutreffen.

5.4.3 Multi-Tenant-Konfiguration

Das Multi-Tenant-Design ist ungleich schwieriger als das Single-Tenant-Design. In einer Multi-Tenant-Konfiguration wird für jede Organisation, die die gleiche vCloud-Automation-Center-Umgebung nutzt, ein neuer Tenant erstellt. User benutzen eine Tenant-spezifische URL zum Einloggen.

Es gibt zwei verschiedene Möglichkeiten für die Konfiguration einer Multi-Tenant-Umgebung:

- Default Tenant MultiTenancy
- Individual Tenant MultiTenancy

Default Tenant MultiTenancy

In diesem Szenario geschieht die meiste Konfiguration zentral im Haupt-Tenant. Dabei werden Fabric Groups und Reservations im Standardmandanten angelegt. Das Anlegen von Business Groups und Blueprints erfolgt jedoch in den einzelnen Mandanten.

Dieses Design eignet sich besonders für mittlere und größer Unternehmen, bei denen die Hardwareressourcen samt vCloud Automation Center zentral verwaltet und zwischen den Tenants geteilt werden, den verschiedenen Geschäftsteilen aber auch eine gewisse Autonomie (mit unterschiedlichen Benutzern und verschiedenen Active Directory-Umgebungen) zugestanden werden soll. Dies umfasst auch die Benutzerverwaltung, da jeder Tenant seine eigene Menge an Identity Stores verwalten kann.

Das Design, wie eine derartige Konfiguration im Haupt-Tenant aussehen kann, ist in Abbildung 5–23 abgebildet.

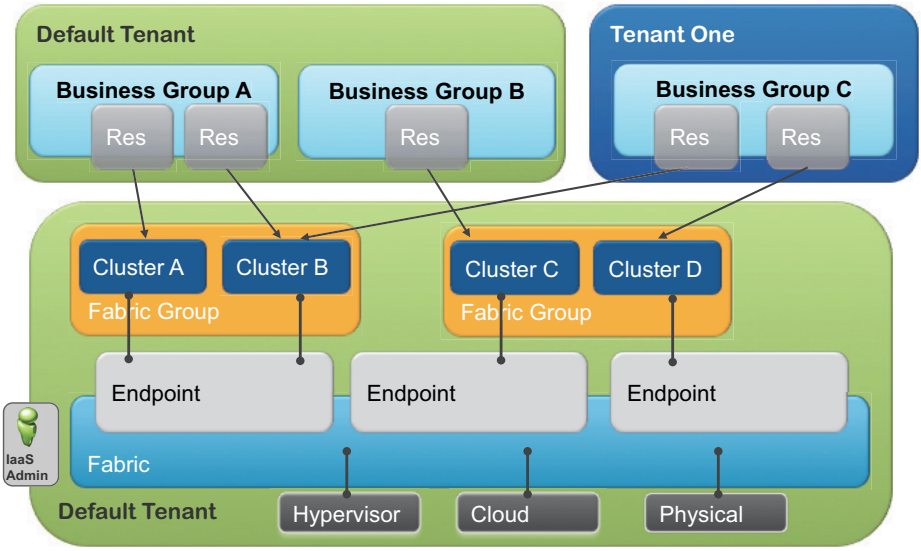

Abb. 5–23 *Konfiguration im Haupt-Tenant*

Die URL-Strategie sollte bei MultiTenancy bekannt sein: Der Login auf dem Standard-Tenant erfolgt über die URL `https://<vrealize-automation-appliance.domain.name>/vcac`, während man bei den einzelnen Tenants die längere URL `https://<vrealize-automation-appliance.domain.name>/vcac/org/<tenantName>` eingeben muss.

Individual Tenant MultiTenancy

Die zweite Strategie für mehrere Tenants lautet Individual Tenant MultiTenancy. Dieses Vorgehen eignet sich insbesondere für große Unternehmen, Rechenzentren oder Cloud-Provider. Mit ihr kann sichergestellt werden, dass keinerlei Hardwareressourcen zwischen verschiedenen Tenants zusammen genutzt werden. Dies bedeutet, dass im Default Tenant lediglich die Endpoints definiert werden. Eine Gruppierung der Hardwareressourcen durch Fabric Groups und alle weiteren Schritte werden jedoch für jeden Tenant separat durchgeführt. Das Design des Individual-Tenant-MultiTenancy-Ansatzes ist in Abbildung 5–24 dargestellt.

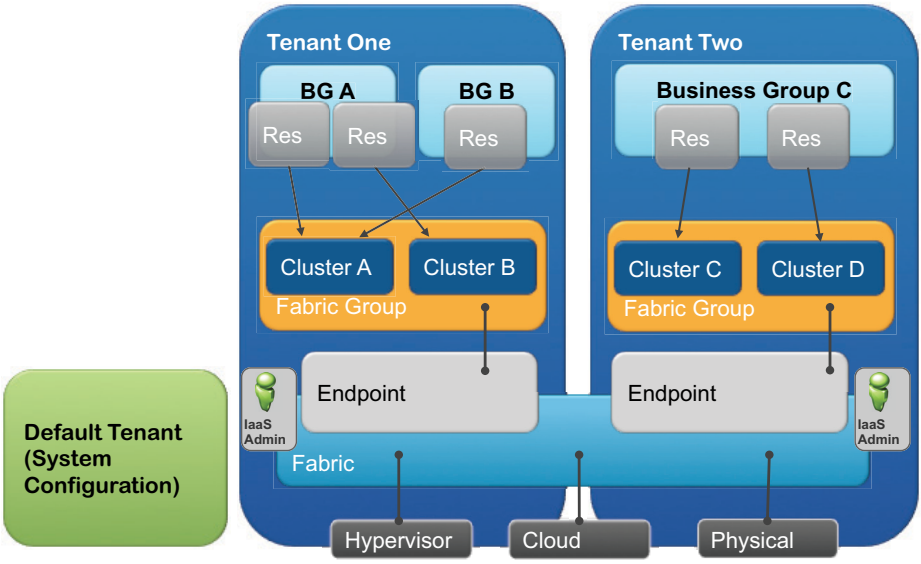

Abb. 5–24 *Individual Tenant MultiTenancy*