Cross-Domain-Security auf Basis von Oracle-Database-Services

Norman Sibbing, ORACLE Deutschland B.V. & Co. KG

Die gängige Praxis, Daten unterschiedlichster Sicherheitsklassen zu speichern beziehungsweise zu verarbeiten, basiert auf dem Prinzip einer galvanischen Trennung der entsprechenden Informationssysteme (Domänen). Dies ist unumstritten die sicherste Variante, Daten zu isolieren.

In physikalisch getrennten Systemen ist es nahezu ausgeschlossen, dass sich Daten höherer Sicherheitsklassen mit Daten niedrigerer Sicherheitsklassen mischen. Personen, die zum Beispiel Zugriff auf Daten der höchsten Schutzklasse haben, müssen allerdings parallel in allen weiteren Domänen der unteren Schutzklassen verwaltet werden. Die Folgen sind hohe Betriebskosten, aufwändige Integration und mangelhafte Flexibilität.

Genau diese drei Punkte nehmen heute an Bedeutung zu, sodass über eine andere Art der sicheren Datenspeicherung unterschiedlichster Datenklassen, gegebenenfalls ohne physikalische Trennung, nachgedacht werden muss. Kosteneinsparungen und Flexibilität durch Verfahrens-/Daten-Konsolidierung und die damit verbundene sichere Datenspeicherung unterschiedlichster Sicherheitsklassen müssen nicht im Widerspruch stehen.

Heutige moderne Sicherheitslösungen bieten Möglichkeiten, einen Kompromiss zwischen Kosten, Flexibilität und Sicherheit zu finden, sofern es keine gesetzlichen Gründe dafür gibt, eine physikalische Trennung der Domänen weiterhin zu betreiben. Aus Sicht der Netzwerke ist eine zumindest logische Trennung durch Virtual Local Area Networks (VLAN) durchaus angebracht. Aus Sicht einer Datenbank lassen sich jedoch praktikablere Lösungen finden als die Verwendung von separater Hardware oder virtueller Maschinen.

Cross Domain Security aus Datenbanksicht

Cross Domain Security auf Basis von Oracle-Datenbank-Services ist ein Lö-

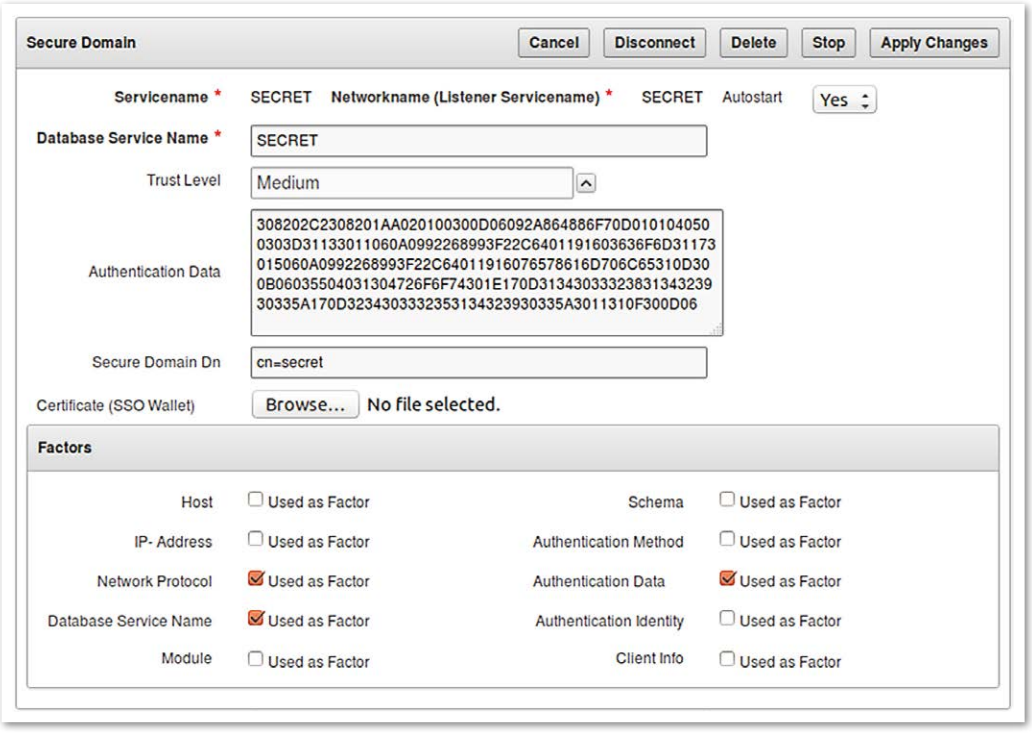

Abbildung 1: Datenbank-Service-Faktor-Mapping

Identities

	Value	Trust Level
▷	TOPSECRET.DUSLNX06.DE.ORACLE.COM	10
▷	SECRET.DUSLNX06.DE.ORACLE.COM	5
▷	CONFIDENTIAL.DUSLNX06.DE.ORACLE.COM	1
▷	PUBLIC.DUSLNX06.DE.ORACLE.COM	-1

Abbildung 2: Trustlevel „DVSYS.GET_TRUST_LEVEL(‚DATABASE_SERVICE')"

sungsansatz, um den anspruchsvollen Anforderungen an Datensicherheit bei gleichzeitiger gemeinsamer Nutzung hochsensibler und weniger sensibler Daten (domänenübergreifend) gerecht zu werden. Er nutzt Oracle Datenbank-Technologien wie Database Vault (DV), Oracle Advanced Security (ASO), Virtual Private Database (VPD) und je nach weiteren Sicherheitsanforderungen auch andere Sicherheits- „Functions and Featues". Sensible Daten werden mit Transparent Data Encryption (TDE) verschlüsselt gespeichert und gemäß strikten, ausgefeilten Sicherheitsregeln (DV) netzwerkübergreifend nutzbar gemacht. Die Kombination aus logischem und physikalischem Zugriffsschutz ermöglicht einen maximalen Schutz vor dem unbefugten Zugriff, selbst durch hochprivilegierte technische Benutzer. Sicherheitseinstufungen (Trustlevel) der Oracle-Clients steuern den Zugriff auf Daten der höchsten Sicherheits-Domäne bis hin auf Daten aller niedriger eingestuften Sicherheits-Domänen, ohne sich dafür bei mehreren Netzwerken anmelden zu müssen (Flexibilität).

Sicherheitseinstufung durch Multifaktor-Autorisierung

Der hier beschriebene Lösungsansatz beruht im Wesentlichen auf dem Prinzip der Multifaktor-Autorisierung des entsprechenden Oracle-Datenbank-Clients. Wichtig ist hier die Verwendung vertrauenswürdiger Client-Faktoren. Diverse Faktoren, die Oracle als Client-Session-Informationen in „SYS_CONTEXT" zur Verfügung stellt, lassen sich bei einzelner Verwendung leicht manipulieren. Nichtsdestotrotz sind sie wertvolle Faktoren zur Steuerung von Zugriffsrechten. Faktoren aus dem Oracle-Client-Session-Kontext wie Programmnamen („program"), Maschinennamen („machine"), Client-Betriebssystem-Benutzer („os_user") und einige weitere lassen sich zwar leicht manipulieren, werden aber durch Kombination mehrerer Faktoren komplexer. Werden diese leicht zu manipulierenden Faktoren durch schwer beziehungsweise gar nicht zu manipulierende Faktoren ergänzt (wie „IP-Adresse" oder „authentication data"), entsteht eine Multifaktor-Autorisierung, die eine verlässliche Identifikation des Oracle-Clients, egal ob „OCI", „Thick JDBC" oder „Thin JDBC", ermöglicht.

Der wichtigste Faktor in der hier dargestellten Lösung ist allerdings der Datenbank-Service-Name. Da jeder Oracle-Client diesen beim Verbindungsaufbau angeben muss und es keinen Sinn ergibt, ihn zu verfälschen, bildet er die Basis des Konzepts. Als positiven Nebeneffekt lassen sich Database-Services wunderbar zur Ressourcen-Steuerung und zum Monitoring verwenden. Bei einem Oracle Real Application Cluster können diese Services dynamisch über mehrere Datenbank-Knoten verteilt gestartet und gestoppt werden.

Ziel ist es, einen Datenbank-Service an mehrere Faktoren (Multi-Faktoren) zu binden. Das bedeutet, wenn ein Oracle-Client einen entsprechenden Datenbank-Service nutzen möchte, muss er alle Faktoren aufweisen, die für die Nutzung des Datenbank-Service erforderlich sind beziehungsweise als notwendig definiert wurden *(siehe Abbildung 1)*.

Hier wird der Datenbank-Service „SECRET" an drei Faktoren gebunden. Das bedeutet, dass der Oracle-Client genau diese Faktoren aufweisen muss, um den Datenbank-Service nutzen zu können:

- Network Protocol
- Authentication Data
- Database Service Name

Diese steuern durch ein Oracle-Database-Vault-Regelwerk die Verwaltung des Benutzerzugriffs auf Daten und Datenbank-Befehle. Zudem wird jedem Datenbank-Service entsprechend einer Daten-Klassifizierung eine Sicherheitseinstufung (Trustlevel) zugeordnet *(siehe Abbildung 2)*. Die Trustlevel selbst sind eine Funktionalität von Database Vault. Alle darin verfügbaren Faktoren (entspricht dem Client-Session-Kontext) lassen sich einem Trustlevel zuweisen. Das bedeutet, dass man den Trustlevel eines Clients in Abhängigkeit seiner Faktoren dynamisch steuern kann. Zu diesen Faktoren gehört der hier verwendete Database-Service-Name, der ja, wie beschrieben, nur nutzbar ist, wenn weitere Faktoren vorliegen.

Autorisierte Oracle-Datenbank-Clients können nun entsprechend ihrer Sicherheits-Domäne auf gekennzeichnete Daten zugreifen, also auf Daten, die der Sicherheitseinstufung (Trustlevel) des Datenbank-Service entsprechen oder einen geringeren Sicherheitsstatus aufweisen *(siehe Abbildung 3)*. Zudem lässt sich mit Oracle Database Vault eine wirksame Aufgabentrennung zwischen sicher-

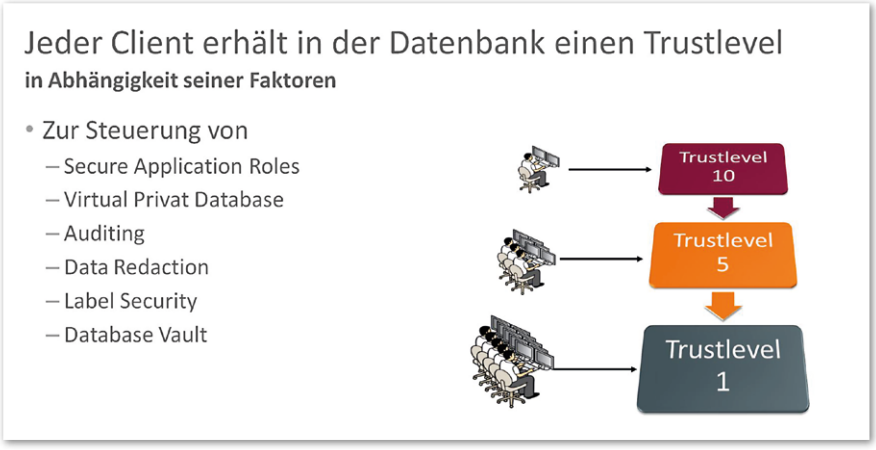

Abbildung 3: Trustlevel

Trustlevel : 10, Database Service Name : * TOPSECRET

	Authentication Identity	Schema	Authentication Method	IP-Address	Host	Network Protocol	Module	Created on
	DBA01	DBA01	PASSWORD	10.200.110.1	NSIBBING-LNX	* TCPS	SQLPLUS	26-MAY-2014 12:51:47

Trustlevel : 5, Database Service Name : * SECRET

	Authentication Identity	Schema	Authentication Method	IP-Address	Host	Network Protocol	Module	Created on
	DEMOAPPS	DEMOAPPS	PASSWORD	10.200.110.1	NSIBBING-LNX	* TCPS	SQLPLUS	02-JUN-2014 13:19:19
	DBA01	DBA01	PASSWORD	10.200.110.1	NSIBBING-LNX	* TCPS	SQLPLUS	26-MAY-2014 13:03:29

Trustlevel : 1, Database Service Name : * SSL

	Authentication Identity	Schema	Authentication Method	IP-Address	Host	Network Protocol	Module	Created on
	DEMOAPPS	DEMOAPPS	* PASSWORD	10.200.110.1	NSIBBING-LNX	* TCPS	SQLPLUS	22-MAY-2014 16:14:39
	CN=NSIBBING,OU=PEOPLE,DC=EXAMPLE,DC=COM	NSIBBING	* SSL	10.200.110.1	NSIBBING-LNX	* TCPS	SQLPLUS	02-JUN-2014 13:39:06

Trustlevel : 0, Database Service Name : * DV01

	Authentication Identity	Schema	Authentication Method	IP-Address	Host	Network Protocol	Module	Created on
	DBA01	* DBA01	PASSWORD	10.200.110.1	* NSIBBING-LNX	TCP	SQLPLUS	27-MAY-2014 13:29:34
	SYSMAN	* SYSMAN	PASSWORD	10.200.110.205	* DBSERVER	TCP	OMS	02-JUN-2014 13:14:47
	DEMOAPPS	* DEMOAPPS	PASSWORD	10.200.110.1	* NSIBBING-LNX	TCP	SQLPLUS	03-JUN-2014 14:20:26

Trustlevel : -1, Database Service Name : * WEBLOGIC

	Authentication Identity	Schema	Authentication Method	IP-Address	Host	Network Protocol	Module	Created on
	DEMOAPPS	* DEMOAPPS	PASSWORD	10.200.110.1	NSIBBING-LNX	TCP	* HR-APPLICATION	05-JUN-2014 09:54:44
	CN=DV01,CN=ORACLECONTEXT,DC=EXAMPLE,DC=COM	* WEBLOGIC_SSO	SSL	10.200.110.1	NSIBBING-LNX	TCPS	* WEBLOGIC-SSO	06-JUN-2014 14:01:20
	DEMOAPPS	* DEMOAPPS	PASSWORD	10.200.110.1	NSIBBING-LNX	TCP	* SQLPLUS	22-MAY-2014 14:50:04

Abbildung 4: Client-Registrierung

heits- und wartungsbezogenen Abläufen durchsetzen. Darüber hinaus dienen die Trustlevel zur Steuerung diverser Oracle-Technologien wie Virtual Privat Database, Auditing, Data Redaction und vieler mehr.

Vorgehensweise

Zunächst muss jeder Oracle-Datenbank-Client gemäß seiner Sicherheits-Domäne von einem Administrator registriert werden, was hier über eine Apex-Applikation erfolgt, und zwar proaktiv über ein Apex-Formular *(siehe Abbildung 4)* durch Eingabe der Client-Faktoren oder reaktiv, nachdem sich ein Client das erste Mal angemeldet hat. In diesem Fall werden die Client-Faktoren vorbelegt. Die Vorgehensweise ist ähnlich wie bei einem WLAN-Router mit MAC-Filter.

Nach erfolgreicher Registrierung des Clients werden beim Aufbau einer Datenbank-Verbindung (Login) alle Client-Faktoren zur Datenbank übermittelt. Diese gesendeten Faktoren werden mit den Werten der ursprünglichen Registrierung verglichen *(siehe Abbildung 5)*. Je mehr Faktoren zur Autorisierung notwendig sind, desto verlässlicher ist die Identifikation des Oracle-Datenbank-Clients.

Sollten die vom Oracle-Datenbank-Client gesendeten Faktoren nicht mit den registrierten Faktoren übereinstimmen, wird der Verbindungsaufbau aufgrund einer Database-Vault-Connect-Regel unterbrochen. Der Client erhält eine Fehlermeldung und wird entsprechend protokolliert *(siehe Listing 1)*.

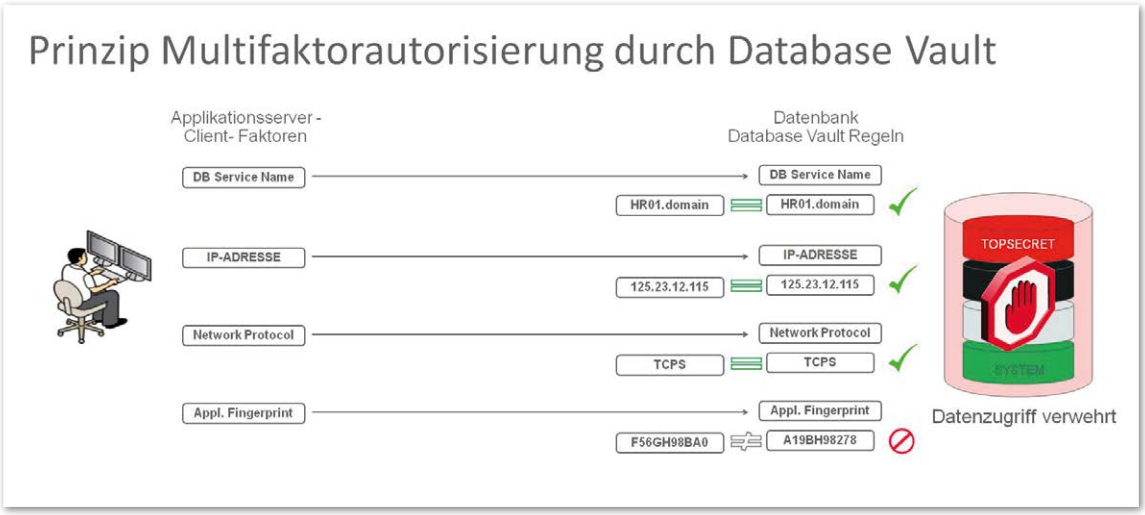

Abbildung 5: Multifaktor-Autorisierung

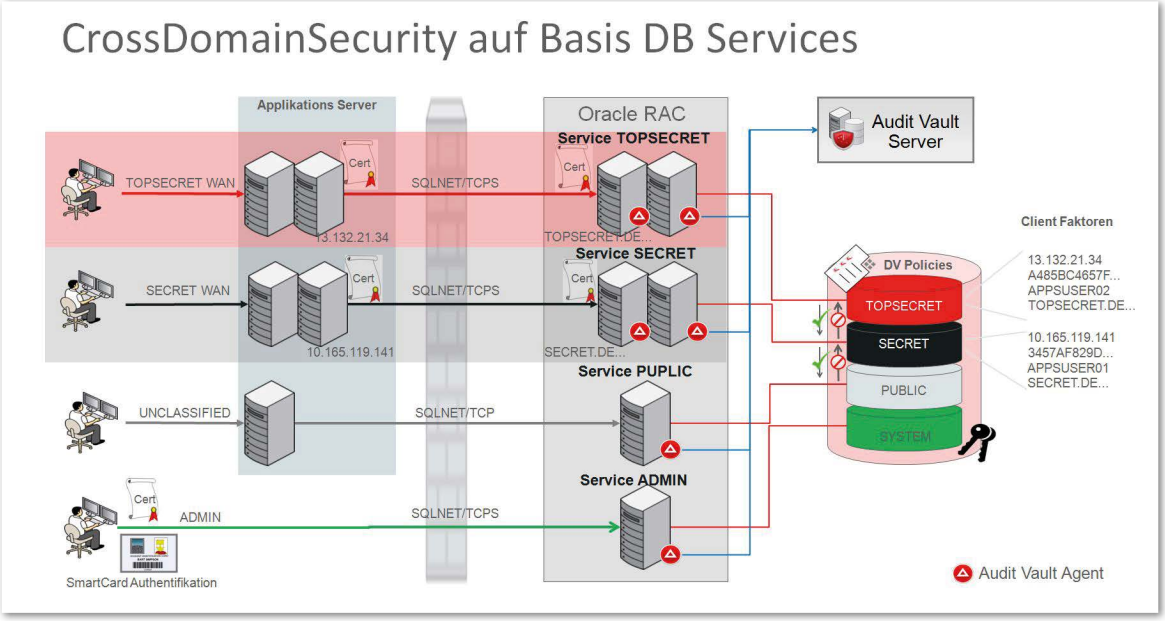

Abbildung 6: Cross-Domain-Security im RAC

Ist der Client erfolgreich authentifiziert und autorisiert, bewegt er sich innerhalb seines Trustlevels beziehungsweise im Trustlevel des Datenbank-Service. Alle weiteren Befugnisse und Zugriffsrechte innerhalb der Datenbank werden durch Standard-Datenbank-Rollen und -Privilegien und/oder weitere Funktionalitäten wie „OLS“, „DV“ oder „VPD“ (gegebenenfalls auf Basis des Trustlevels) gesteuert. Eine weitere Rechte-Vergabe über Rollen lässt sich über die Verwendung von Secure-Application-Rules steuern.

Fazit

Dieser Lösungsansatz ermöglicht es den Datenbank- beziehungsweise Sicherheits-Administratoren, die Kontrolle darüber zu bewahren, welche Clients aus welchen Netzen und mit welchen Tools beziehungsweise Applikationen auf die Datenbank zugreifen. Die Kontrolle des initialen Verbindungsaufbaus eines Clients bildet somit eine weitere Sicherheitsebene. Clients lassen sich dynamisch sperren und entsperren. Dies kann ad hoc oder zeitlich gesteuert geschehen. Die hier vorgestellte Lösung lässt sich gemäß den Anforderungen leicht anpassen.

Bei einer Konsolidierung von Daten unterschiedlicher Datenschutz-Klassen in eine Datenbank ist die Verwendung eines Oracle-Datenbank-Clusters (RAC) von enormem Vorteil. Zum einen lässt sich so die Verfügbarkeit und Performanz der Datenbank-Services gewährleisten, zum anderen besteht die Fähigkeit, sensible Daten nur auf dedizierten (gemäß der Schutzklasse der Daten) Cluster-Knoten zu betreiben. Hierzu werden entsprechende Datenbank-Services für höher sensible Daten ausschließlich auf Cluster-Knoten gestartet, die besonders dafür ausgelegt sind (spezielle Härtung, Auditing, Benutzer etc.). Damit lässt sich gewährleisten, dass sich keine sensiblen Daten im Hauptspeicher (SGA) der Cluster-Knoten befinden, die einer niedrigeren Sicherheitsstufe (Trustlevel) entsprechen *(siehe Abbildung 6)*. Gleichzeitig lassen sich aber auf Cluster-Knoten höherer Sicherheitsstufen Daten der niedrigeren Sicherheitsstufen verarbeiten.

Der hier dargestellte Lösungsansatz zur Konsolidierung von Daten unterschiedlichster Schutzklassen zeigt auf, dass moderne technologische Möglichkeiten existieren, die den Kompromiss finden zwischen Kosteneinsparungen und Flexibilität durch Verfahrens-/Daten-Konsolidierung und die damit verbundene sichere Datenspeicherung unterschiedlichster Sicherheitsklassen, sofern es keine gesetzlichen Vorschriften gibt, eine physikalische Trennung der Domänen weiterhin zu betreiben.

```
[nsibbing@secret]$sqlplus demoapps/abcd1234@topsecret
SQL*Plus: Release 11.2.0.2.0 Production on Fri Apr 5 11:41:35 2013
Copyright (c) 1982, 2010, Oracle.   All rights reserved.
ERROR:
ORA-47306: 20222: Client is not registered
```

Listing 1

Norman Sibbing
norman.sibbing@oracle.com