MultiTenancy - An Overview For Techies

Timothy D. Kuehn
Senior OpenEdge Consultant
TDK Consulting Services Inc

timk@tdkcs.ca tim.kuehn@gmail.com
Ph 519-576-8100 Cell: 519-781-0081

MultiTenancy for Developers

PUG Challenge 2013 - Recommended Sessions

TDK Consulting Services Inc

- Programming with the Client-Principle Object -- Chris Longo
- Basics of Identity Mgmt in OpenEdge (Part I) -- Peter Judge
- Coding with ID Mgmt and Security (Part II) -- Peter Judge
- Server Access - The REST of the Story -- Mike Jacobs

MultiTenancy For Developers
Storage Area Structures

TDK Consulting Services Inc

Type I:

- Inventory Data
- Inventory Index
- Order Data
- Order Data
- Order Index
- Inventory Index
- Inventory Data

Type II:

- Cluster
  - Inventory Data
  - Inventory Data
- Cluster
  - Inventory Index
  - Inventory Index
- Cluster
  - Inventory BLOB
  - Inventory BLOB

MultiTenancy For Developers
Storage Structures

TDK Consulting Services Inc

MultiTenant Table in Type II Storage Area

Tenant: Coyote

Inventory Data	Inventory Data	Inventory Index	Inventory Index	Inventory BLOB	Inventory BLOB
Cluster		Cluster		Cluster	

Tenant: Road Runner

Inventory Data	Inventory Data	Inventory Index	Inventory Index	Inventory BLOB	Inventory BLOB
Cluster		Cluster		Cluster	

Tenant: Balto

Inventory Data	Inventory Data	Inventory Index	Inventory Index	Inventory BLOB	Inventory BLOB
Cluster		Cluster		Cluster	

MultiTenancy For Developers
Storage Structures

TDK Consulting Services Inc

MultiTenant Groups

Tenant: Coyote

Inventory

Viewers

Tenants in a group share access to a single data partition of the "viewers" table

Tenant: Road Runner

Inventory

All tenants have their own distinct "inventory" table partition

Tenant: Balto

Inventory

Viewers

Since Balto is not a group member, he gets his own "viewers" partition.

What happens when a group has no tenant members….

Viewers

MultiTenancy For Developers
Storage Structures

TDK Consulting Services Inc

Shared Tables

Tenant: Coyote

Inventory

Tenant: Road Runner

Inventory

Viewers

Geographic Information System Data

Everyone sees and updates the same table at the same time

Tenant: Balto

Inventory

Viewers

MultiTenant Tables

Shared Tables

MultiTenancy For Developers
Database Sequences

TDK Consulting Services Inc

- “Global Shared Sequence” -> Same as current sequence, all tenant users see the same value
- “MultiTenant Sequence” -> Each tenant gets their own sequence

MultiTenancy For Developers Database Sequences

TDK Consulting Services Inc

MT Sequence

Tenant: Coyote

Inventory ID

Tenant: Road Runner

Inventory ID

All other Tenants:

Inventory ID

Each tenant gets their own counter.

Each tenant's counter increments independent of all other tenant's counters

Global Shared Sequence

Viewer ID

The counter increments at the same time and has the same value for all tenants

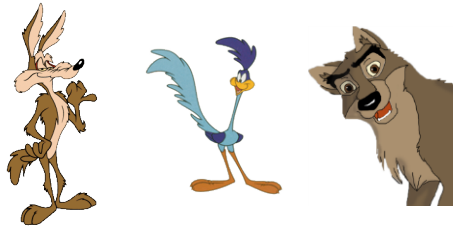
MultiTenancy For Developers (Security) Domains

TDK Consulting Services Inc

Domains -

Are collections of users within a tenant

Determines which tenant's data a user has access to



Determines how users are authenticated

Controls user access

MultiTenancy For Developers (Security) Domains

TDK Consulting Services Inc

Domain Rules:

- Must be associated with a database tenant
- Must be unique across all database tenants
- Must have an authentication configuration
- The “” (blank) domain is the ‘default’ domain
- Names can be up to 64 chars long

MultiTenancy For Developers
Domains

TDK Consulting Services Inc

Tenant: Coyote

Domains

- research.coyote.com
- fabrication.coyote.com

Tenant: Road Runner

- research.roadrunner.com
- tactics.roadrunner.com

Inventory

Inventory Sequence

Inventory

Inventory Sequence

Viewer

MultiTenancy For Developers Users

TDK Consulting Services Inc

User Rules -

- Are identified within a domain
- Must be unique within domain
- Can have the same name in multiple domains (even within the same tenant)

Best Practices:

- Match development login user tenant with the type of user who'll be using the data

MultiTenancy For Developers
Users

TDK Consulting Services Inc

User@Domain

Tenant: Coyote

secret@research.coyote.com

welder@fabrication.coyote.com

Tenant: Road Runner

secret@research.roadrunner.com

survival@tactics.roadrunner.com

Inventory

Inventory Sequence

Inventory

Inventory Sequence

Viewer

MultiTenancy For Developers
Authentication

Authentication is the process performed by an *authentication system to validate a user's asserted* identity and determine their abilities and rights to access data sources.

Authentication process is defined at the domain level.

- _oeusertable: Authenticate using the _user table (-U –P)
- _oslocal: Authenticate using the OS
- _extsso: External Single Sign-on
- {userdefined}: 11.0 -> same as _extsso, 11.1: SSO & ABL

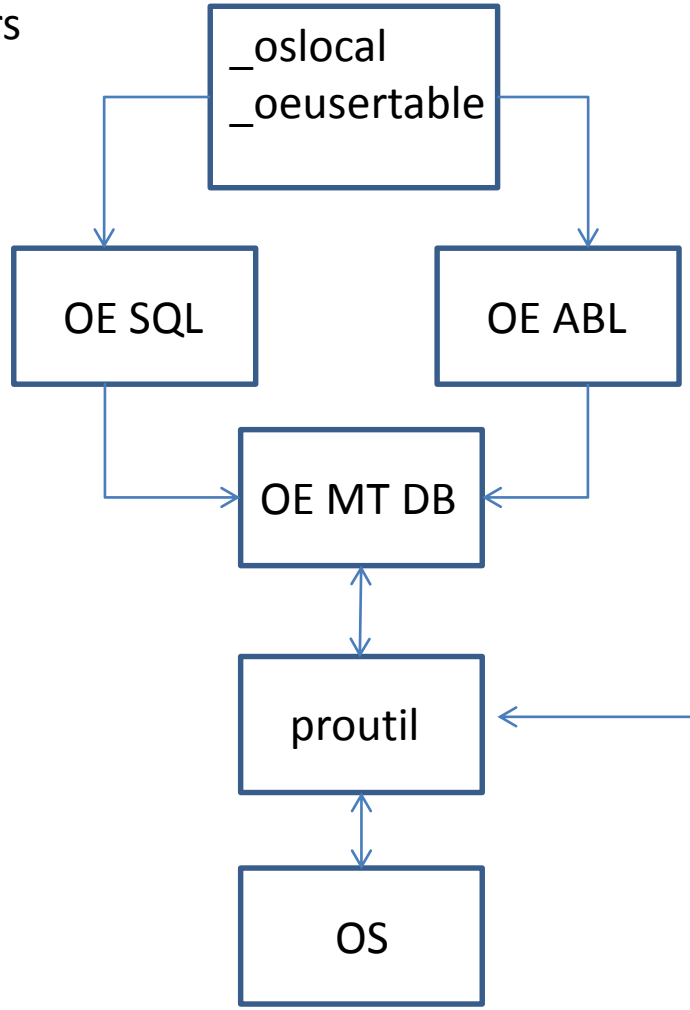
Notes:

- _user can be configured for access by SQL92 only
- _oslocal executes whever the AVM session runs

MultiTenancy For Developers Authentication

TDK Consulting Services Inc

Authentication layers



Can authenticate using the OS identity or the _user table

How does the AVM know when a session has been authenticated?

MultiTenancy For Developers
Client-Principal

Client-Principal: A security token containing trusted user credentials that establish user identity for an ABL session and database connection(s).

Types of CP objects:

Type	Description
Unsealed	The CP object information has not been authenticated and can be changed. (See the "LOGIN-STATE" attribute for more details)
Sealed	CP object values have been set to authenticate access to the user@domain's tenant, then converted to a tamper-proof token that can't be changed.

MultiTenancy For Developers
Establishing a Session

TDK Consulting Services Inc

Receive login information

Authenticate

Create sealed CP object

Return session token

Create session token

Store CP object in a safe place

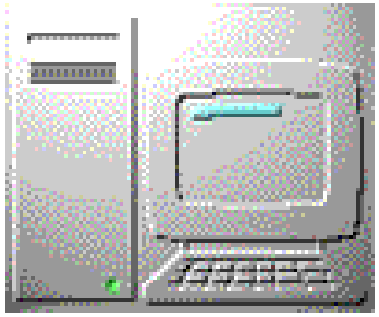
MultiTenancy For Developers
Session Service Call

TDK Consulting Services Inc

Pass session token to service

Validate session token

Get session's CP object



Return results to caller

Perform work

Assert identity

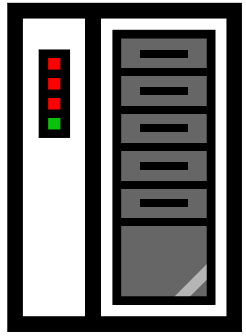
MultiTenancy For Developers
Remote Session Server Call

TDK Consulting Services Inc

Pass session token to service

Validate session token

Get session's CP object



Return results to caller

Perform work

Assert identity

Pass CP to remote server

MultiTenancy For Developers
Using Client-Principal to Establish Tenancy

TDK Consulting Services Inc

```
RUN Authenticate.p(user-id, domain, userpassword, OUTPUT is-ok).
IF NOT is-ok THEN LEAVE.
CREATE CLIENT-PRINCIPAL hCP.
hCP:INITIALIZE(user-id + "@" + domain).
hCP:SEAL(DomainAccessCode).

IF is-remote THEN
  op-raw = hCP:EXPORT-PRINCIPAL().

IF is-local THEN
  SET-DB-CLIENT(hCP).
```

See _Domain._Domain-Access-Code

For more on the CP object, see "OE Getting Started: Core Business Services" page 4-9ff

MultiTenancy For Developers
What happens on identity switch?

TDK Consulting Services Inc

Tenant: W.E. Coyote

welder@fabrication.coyote.com

Tenant: RoadRunner

secret@research.roadrunner.com

MultiTenancy For Developers
What happens on identity switch?

TDK Consulting Services Inc

welder@fabrication.coyote.com
Tenant: W.E. Coyote

secret@research.roadrunner.com
Tenant: RoadRunner

Tenant Tables and Sequences

Tenant Tables and Sequences

Viewers

Geographic Information System Data

MultiTenancy For Developers
What happens on identity switch?

TDK Consulting Services Inc

owner@balto.com
Tenant: Balto

Tenant Tables and Sequences

Viewers

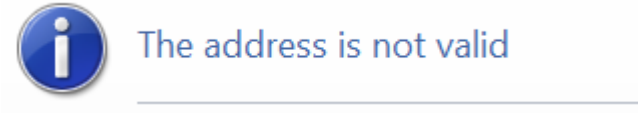
Geographic Information System Data

MultiTenancy For Developers
What happens on identity switch?

TDK Consulting Services Inc

Other things remember:

- All database buffers and queries are invalidated



- Prodatasets, temp tables, variables, and shared variables retain their state
- Prodatasets, temp-tables, and variables do NOT track tenant identity

MultiTenancy For Developers the story continues…

TDK Consulting Services Inc

MultiTenancy For Developers
How can tenants share data?

TDK Consulting Services Inc

The Riddler has a riddle for you…

Tenant: Coyote

Inventory

Tenant: Road Runner

Inventory

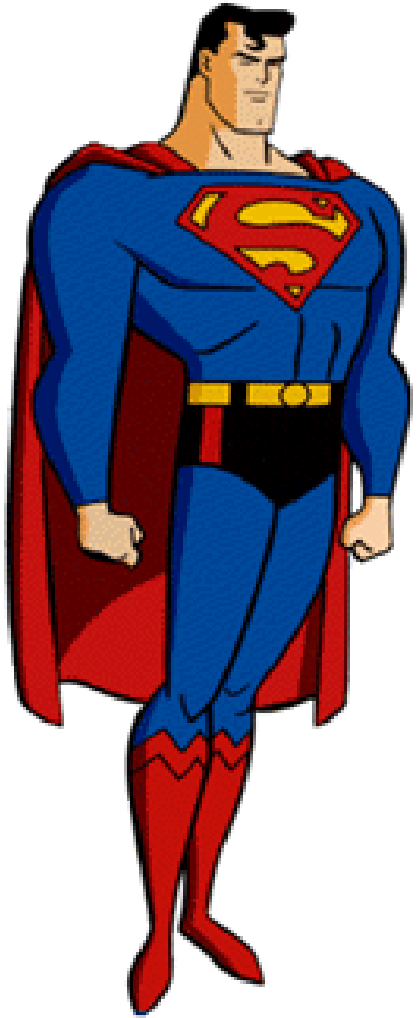
Tenant: Balto

Inventory

Viewers

MultiTenancy For Developers
Introducing the Supertenant

TDK Consulting Services Inc



MultiTenancy For Developers
Finding the Supertenant

TDK Consulting Services Inc

Tenant: Coyote

Inventory

Viewers

Tenant: Road Runner

Inventory

Tenant: Balto

Inventory

Viewers

Tenant: Default

Inventory

Viewers

Tenant: Super

Effective Id defaults to "default" tenant on login

MultiTenancy For Developers
Creating and Using the Supertenant

TDK Consulting Services Inc

1. Create a “Super” Tenant
2. Create a security domain in the super tenant
3. Create a user in the super tenant domain
4. Login and do work

Table: _Tenant

Field	Descr
_Tenant-Name	Unique name for tenant
_TenantID	System applied ID. < 0 -> Super Tenant, = 0 -> Default Tenant, > 0 -> Regular Tenant
_Tenant-Description	User entered description
_Tenant-Type	Internal Use
_Tenant-Attributes[64]	PSC Used Flags
_Tenant-Data-Area-Default	Default storage area for data
_Tenant-Index-Area-Default	Default storage area for indexes
_Tenant-Lob-Area-Default	Default storage area for LOBs
_Tenant-Sequence-Block	Storage area for sequences

Table: _sec-Authentication-Domain

Field	Descr
_Domain-Name	Name of the security domain
_Domain-Type	Internal Use
_Domain-Enabled	Is domain enabled for user access?
_Auditing-Context	User supplied information recorded in the auditing's _auditing-context field
_Domain-Access-Code	Used to validate the CP authenticity "seal" before it will be used and used to verify that the CP has access to the current domain
_Tenant-Name	Same as _Tenant._Tenant-Name

MultiTenancy For Developers
Being the Supertenant: VSTs

TDK Consulting Services Inc

Table: _User

Field	Descr
_UserID	System assigned ID
_Domain-Name	Name of the Domain this user belongs to
_User-Name	Name of the user
_Password	User's Password
_TenantID	Same as _Tenant._TenantID

Note: _user's primary index has changed to _userid + _domain_name

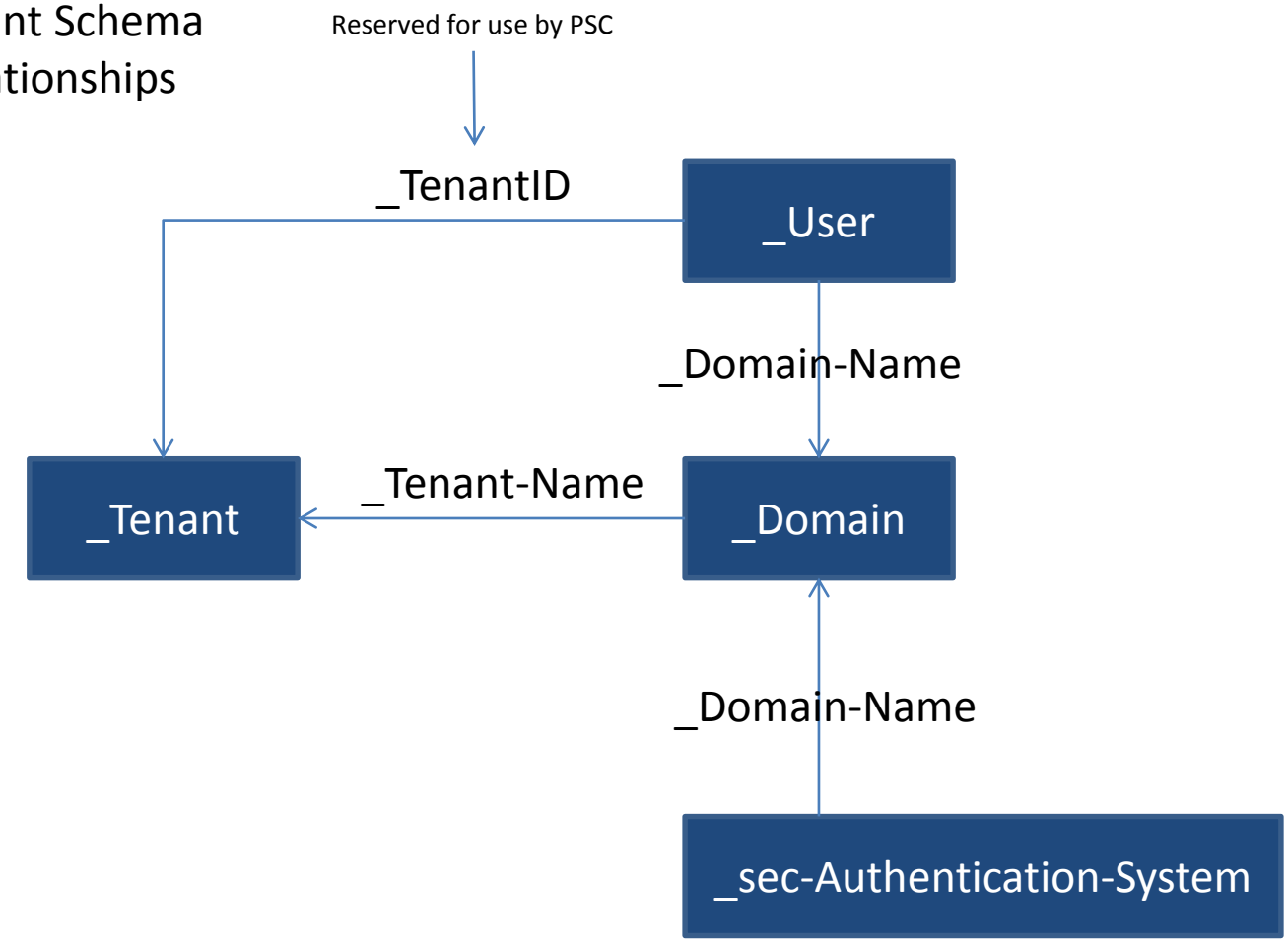
Table: _sec-Authentication-System

Field	Descr
_Domain-Name	Name of domain that uses this system
_Domain-Type	Used internally to link _sec-authentication-domain to _sec-authentication-system
_PAM-Module-Name	Designates the authentication system that supports authentication to user accounts using external user account software
_PAM_Callback_Procedure	Path to the ABL procedure to run when OE performs user authentication / SSO inside of SET-DB-CLIENT() and SECURITY-POLICY:SET-CLIENT()

MultiTenancy For Developers
Being the Supertenant: VST Relationships

TDK Consulting Services Inc

MultiTenant Schema
Table Relationships



Also: _partition-set and _partition-set-detail – See MT Abl pg 213

MultiTenancy For Developers
Being the Supertenant: Language Additions

TDK Consulting Services Inc

Language Element	Type	Notes
IS-DB-MULTI-TENANT()	Function	
IS-MULTI-TENANT	Property	
SET-EFFECTIVE-TENANT()	Function	Does not invalidate current buffers, Undo does not reset EFF TNT
GET-EFFECTIVE-TENANT-ID()	Function	
GET-EFFECTIVE-TENANT-NAME()	Function	
TENANT-NAME-TO-ID()	Function	Convert Tenant Name to an ID
TENANT-ID()	Function	DB connection tenant ID
TENANT-NAME()	Function	DB connection tenant Name
CREATE … FOR TENANT	Statement	Create record for specific tenant
BUFFER-CREATE	Method	Create record for specific Tenant

See Chapter 3: MultiTenant OE Development Programming Interfaces

MultiTenancy For Developers
Being the Supertenant: Language Additions

TDK Consulting Services Inc

Language Element	Type	Notes
BUFFER-TENANT-ID	Attribute	Associated with a buffer
BUFFER-TENANT-ID()	Function	Associated with a buffer
BUFFER-TENANT-NAME	Attribute	Associated with a buffer
BUFFER-TENANT-NAME()	Function	Associated with a buffer
REPOSITION qrynme TO ROWID	Attribute	Can reposition a query to a rowID in a tenant table
REPOSITION query TO ROWID()	Method	Can reposition a query to a rowID in a tenant table
TENANT-WHERE	Clause	Used in a FOR EACH to read records from multiple tenants
SKIP-GROUP-DUPLICATES	Clause	Process a GROUP table once

See Chapter 3: MultiTenant OE Development Programming Interfaces

MultiTenancy For Developers
Being the Supertenant: MakingThingsEasier

TDK Consulting Services Inc

MT API

MultiTenancy For Developers
Being the Supertenant: Things to Remember!

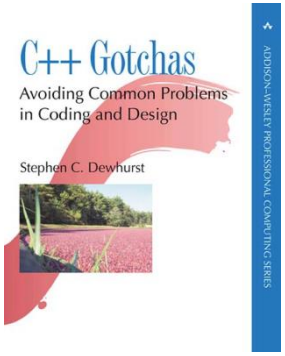
TDK Consulting Services Inc

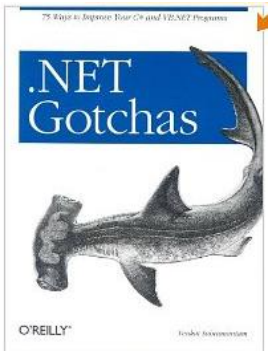
Things to remember:

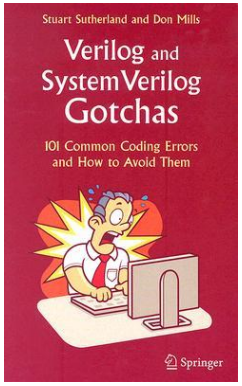
1. Each tenant's partition is distinct, so table key values will be unique for a tenant/group and a table only
2. ROWID's are unique to a tenant and area *only*.
3. Each record of a MT table has an identifier can be used to link it to a tenant via a BUFFER-TENANT-* call/reference
4. Tenant ID, like ROWID and RECID, is not guaranteed to remain the same across a D&L or tenant migration, and should only be used within a single AVM session.

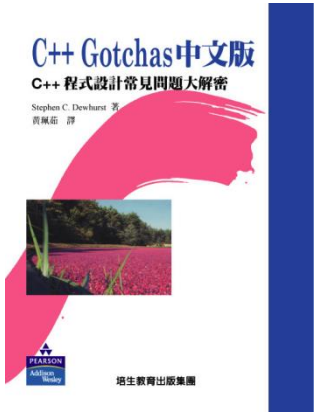
MultiTenancy For Developers
MT and Super Tenant Gotcha's

TDK Consulting Services Inc





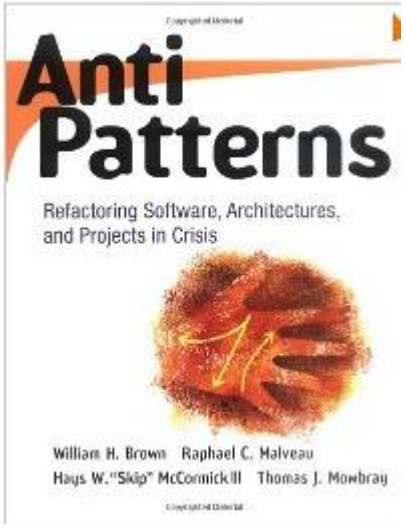




Top 5 "Gotchas" To Avoid

When Implementing Identity Resolution

Request Your Complimentary Copy



MultiTenancy For Developers
MT and Super Tenant Gotcha's

TDK Consulting Services Inc

Requires ability to map single application structures to meta-application structures

Tenant: Coyote

Inventory

Tenant: Road Runner

Inventory

Tenant: Balto

Inventory

Viewers

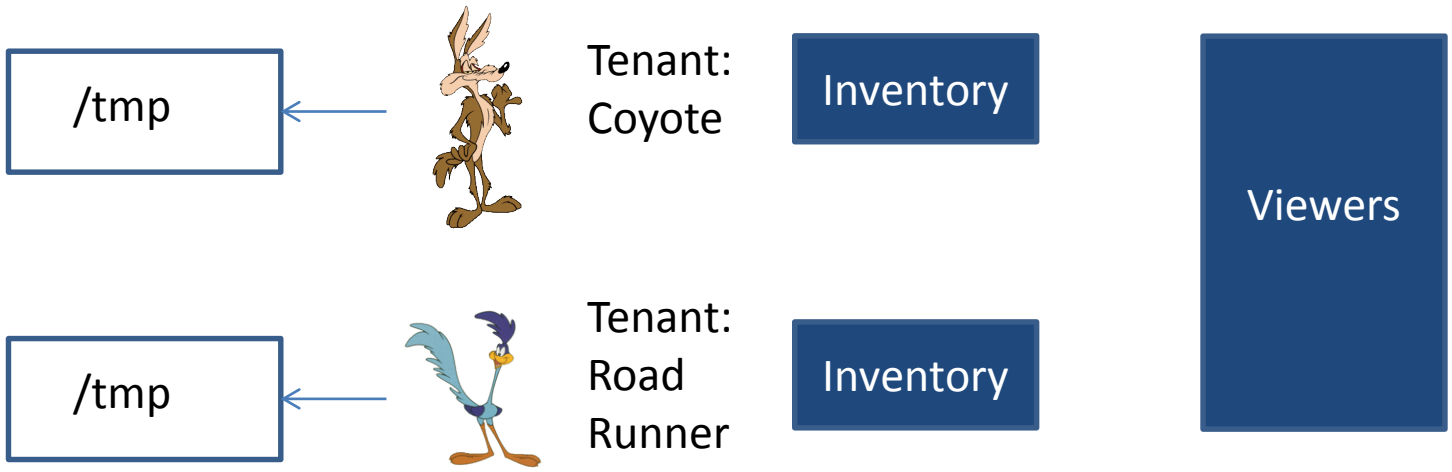
Viewers

Geographic Information System Data

MultiTenancy For Developers
MT and Super Tenant Gotcha's!

TDK Consulting Services Inc

External file, directory, and service collision avoidance



MultiTenancy For Developers
The Riddler Says: Questions Anyone?

TDK Consulting Services Inc

Questions…?

MultiTenancy For Developers
Thank you for your time!

TDK Consulting Services Inc

This presentation brought to you by:

Tim Kuehn
Senior OpenEdge Consultant
TDK Consulting Services Inc.
519-576-8100 tim.kuehn@gmail.com