Sistema Informativo Territoriale per la Regione Autonoma della Sardegna (SITR – IDT)

Razionalizzazione utenze

Data emissione	11/05/2010
Codice(revisione)	A
Emesso da:	XXXXXXXX
Verificato da:	XXXXXXXX
Approvato da:	XXXXXXXX
Protocollo consegna:	SITR-COM-1011

Title/Titolo	Razionalizzazione utenze
Creator/Creatore	XXXXXXXX
Date/Data	11/05/2010
Subject/Soggetto	Razionalizzazione utenze
Type/Tipo	Testo
Publisher/Editore	Regione Autonoma della Sardegna
Description/Descrizione	Il documento descrive il piano di lavoro per la gestione dei metadati e delle foto aeree
Contributor/Autori	XXXXXXXX
Format/Formato	MS Word 2003 (.doc)
Source/Riferimento	Nessuno
Rights/Diritti	Regione Autonoma della Sardegna
Identifier/Identificatore	SITR-INT-004
Language/Lingua	Italiano
Relation/Relazioni	Nessuna
Coverage/Durata ed estensione	Durata del progetto

INDICE DEGLI ARGOMENTI

INDICE DELLE TABELLE

INDICE DELLE FIGURE

STORIA DELLE REVISIONI

Revisione	Data	Autore/i	Modifiche
A	26/01/2010	XXXXXXXX	Prima stesura

CONVENZIONI SULLA NOMENCLATURA DELLA DOCUMENTAZIONE

Il nome dei documenti è costituito dalle seguenti sezioni separate da trattino ("-"):

SITR-XXX-nnn(Y) – <descrizione>

SITR	codice fisso indicante l'appartenenza al progetto SITR
XXX	codice letterale di 3 caratteri indicante la categoria di documento
nnn	progressivo univoco all'interno della categoria di documento
(Y)	codice letterale di 1 carattere indicante la revisione
<descrizione>	descrizione in linguaggio naturale

1. Introduzione

L'attività descritta in questo documento mira a fotografare l'attuale gestione della sicurezza nel perimetro dell'Infrastruttura di Dati Territoriali del SITR. Verranno individuate anche le azioni da mettere in campo immediatamente nell'ipotesi, però, di non avviare alcuno sviluppo evolutivo del software esistente. Tali interventi si dovranno quindi limitare alla riconfigurazione di tali applicazioni o attività sistemistiche su software di base. Si sottolinea che risultati ottenuti con questi interventi non consentiranno di ottenere una centralizzazione dei meccanismi di Autenticazione/Autorizzazione né ottenere una sincronizzazione dei repository utenti attualmente presenti nella IDT, quantomeno l'attivazione di soluzioni di Single Sign On. Quello che si vuole raggiungere è bonificare le eventuali situazioni anomale e aumentare il livello di sicurezza, ma sempre nello scenario di mantenimento dei sistemi esistenti e non tenendo in considerazione delle problematiche di mantenimento del sistema.

E' prevista anche l'introduzione di una Directory utenti conforme al protocollo LDAP (individuata al momento nel OSS OpenDS o in Microsoft Active Directory già presente nei server Windows 2003) dove inserire le nuove utenze individuate. Tale Directory non potrà essere però utilizzata come sistema di identificazione considerati le limitazioni di intervento sulle applicazioni/servizi da mettere in sicurezza.

Nel perimetro di intervento di questa attività ricade solamente ciò che è compreso dentro i confini della IDT, ma il censimento è esteso comunque a tutto il SITR. Nell'attività di identificazione delle entità, si considera inoltre solo l'ambiente di produzione e non quello di test/collaudo.

Di seguito alcuni approfondimenti dei punti fissati nell'analisi preliminare.

1.1. Utilizzo di utenti personali

La IDT del SITR prevede nella sua architettura tre tipi di accesso al dato geografico:

- Accesso tramite applicazioni
- Accesso tramite servizi
- Accesso diretto

Proprio quest'ultima tipologia di canale di accesso ai dati (che si traduce nella possibilità per l'utente di connettersi con un proprio client GIS direttamente al database Oracle o al FileSystem dove è materialmente implementato il *GeoRepository* dell'infrastruttura) ha indotto a ipotizzare, ai fini di una corretta gestione del controllo degli accessi, l'utilizzo di "utenti personali" laddove la tecnologia in uso lo consenta.
Questa scelta si traduce nella definizione all'interno del DBMS (nonché del dominio Windows a cui è delegato il controllo degli accessi al FileSystem) di un utente Oracle per ciascun utente fisico dell'infrastruttura. Ovviamente una condizione necessaria per questa soluzione è la coincidenza dei domini (o reale o virtuale mediante sincronizzazione).

Sempre come scelta architetturale della IDT, i dati geografici vettoriali sono mantenuti in un unico SCHEMA (utente proprietario) di nome IDT in tabelle o viste geografiche (al momento vengono utilizzate solamente tabelle); il meccanismo di gestione del dato spaziale Oracle prevede che per ciascuno di essi esista un record di metadati nella vista **ALL_SDO_GEOM_METADATA.** Senza tali metadati (dove sono registrati, ad esempio, extent spaziale, sistema di riferimento di coordinate, quali sono le colonne geometriche …) non è possibile utilizzare correttamente i dati geografici della tabella/vista corrispondente.
Gli utenti al fine di registrare un dato spaziale devono popolare questa vista e ciò avviene indirettamente, attraverso la gestione di un'altra vista su cui hanno i diritti di scrittura, **USER_SDO_GEOM_METADATA;** questa vista è fatta in modo tale da filtrare solamente i metadati degli oggetti spaziali di cui l'utente è proprietario.
Le registrazioni nel nostro caso avvengono tutte da parte dell'utente IDT.
Nella nostra ipotesi, dove gli utenti di consultazione accedono con un utente Oracle che non possiede alcuna tabella spaziale (ma che ha i necessari diritti di lettura sulle tabelle dello schema IDT), tutte le viste **USER_SDO_GEOM_METADATA** non possiedono alcun record, esclusa quella dell'utente IDT.

Ricordiamo inoltre che non è possibile inserire più record relativi alla medesima tabella dello schema IDT, con utenti diversi da IDT poiché l'attributo OWNER (è quello che contiene lo schema proprietario della tabella spaziale) della tabella sottostante alla vista **USER_SDO_GEOM_METADATA** non è compreso nella primary key della tabella stessa.

Questa situazione di per sé non comporta problemi (se non quello secondario di non potere avere tabelle spaziali con lo stesso nome e con lo stesso nome della colonna spaziale in schemi differenti, ma questo è un limite dell'architettura Oracle SDO), ma alcuni client GIS quando si collegano al DB Oracle propongono solo il contenuto della vista **USER_SDO_GEOM_METADATA** e non eseguono il browsing di **ALL_SDO_GEOM_METADATA** (filtrandolo ovviamente in base ai diritti di SELECT sulle tabelle spaziali relative) con la conseguenza, nel nostro caso, di non mostrare alcun dato disponibile.

In particolare questo problema è presente nel datastore Oracle della libreria Geotools per le versioni inferiori alla 2.5.8. I client che ne fanno uso sono GeoServer e uDig, ma mentre in Geoserver dalla versione 1.7.7 compresa si utilizza GeoTools v.2.5.8 o superiore, nell'attuale versione di uDig (v.1.1) il baco è presente utilizzando ancora GeoTools v.2.2.3 (la versione attuale di GeoTools è 2.6.3).

A parte questi dettagli, si conferma quindi quanto previsto nell'analisi preliminare e cioè le seguenti scelte progettuali:

- Tutte i dati geografici vettoriali del DB Unico risiederanno come viste e/o tabelle nello schema dell'utente IDT;
- Le tabelle/viste spaziali risulteranno quindi registrate nei metadati di Oracle a nome dell'utente IDT;
- Gli utenti personali che avranno diritto all'accesso diretto via connessione Oracle alle tabelle spaziali dovranno utilizzare client GIS che si basano sulle reali abilitazioni di accesso ai dati e non a quanto registrato nelle viste personali (che saranno sempre vuote).

1.2. Accesso diretto al DB

Le tabelle/viste spaziali Oracle possono essere accedute direttamente in due modalità differenti:

- in connessione diretta vera e propria (il client utilizza i metadati nativi SDO)
- tramite connessione ArcSDE (il client utilizza i metadati del catalogo SDE oltre alle eventuali strutture dati ausiliarie come indici).

La connessione SDE in origine non poteva essere considerata una connessione diretta, ovvero una connessione dove tra client e server Oracle non si interpone nulla. Essa, infatti, prevedeva l'installazione di software lato server con la funzione di gateway per i client verso il DB. Nel tempo, l'evoluzione del software ArcSDE, ha inglobato nel codice dei client la componente server per cui si può considerare la connessione diretta a tutti gli effetti.

Ovviamente i client ESRI utilizzano questa modalità come meccanismo di connessione di default.

Analogamente alla registrazione su Oracle, per registrare un oggetto spaziale sul catalogo SDE (ovvero creare i metadati necessari alla connessione) si utilizzano una serie di utility fornite con il software ArcSDE; in particolate per creare un record nel catalogo SDE si utilizza il comando:

```
sdelayer –o register …
```

Per definirne i privilegi si usa invece:

```
sdelayer –o grant -A <SELECT,UPDATE,INSERT,DELETE> …
```

I privilegi si mappano 1:1 con i privilegi degli oggetti spaziali Oracle, ma essi vengono rilasciati anche su oggetti ausiliari di SDE presenti sul DBMS.

Una grant SDE comprende quindi una equivalente grant ORACLE, nel senso che eseguendo il comando per una grant SDE su di una tabella spaziale vengono assegnati anche i privilegi necessari per fruire del dato spaziale tramite una connessione diretta semplice. Non è vero invece il viceversa.

Per potere essere registrata nel catalogo SDE, una tabella spaziale Oracle deve quindi soddisfare i seguenti requisiti:

- Deve appartenere all'utente che registra la tabella
- Deve possedere una sola colonna di tipo SDO_GEOMETRY
- Non deve avere altre colonne con tipo definito dall'utente
- Deve essere catalogato in SDO (deve esserci un record valido in USER_SDO_GEOM_METADATA)
- Deve avere una singola tipologia di geometria (punti, linee o poligoni). Sono ammesse geometrie multiparte.
- Deve possedere una colonna adatta per essere registrata come "row ID column", cioè INTEGER, UNIQUE, NOT-NULL

- Deve avere un indice spaziale
- Deve aver passato i test di validazione geometrica di Oracle

Ai fini della sicurezza quindi una risorsa costituita da una tabella/vista spaziale Oracle può avere una duplice interfaccia di accesso: Oracle e SDE.

Si ritiene quindi opportuno introdurre anche il tipo di risorsa "sde" indicando con questa un oggetto spaziale Oracle inserito nel catalogo SDE accessibile attraverso un client SDE..

1.3. Servizi e layer TMS

La IDT utilizza una modalità efficace per servire immagini georeferenziate via web ottimizzata per i client di tipo "tiled". Tale modalità va sotto il termine TMS (Tiled Map Service) e anche se non è un protocollo standard è sufficientemente diffuso per considerarlo un standard de facto. Questo tipo di servizio ha la particolarità di fornire un solo layer per volta e le immagini relative devono essere pre-renderizzate e organizzate in tasselli.
Per modellare questa tipologia di dati e servizi dal punto di vista della sicurezza (anche se nativamente non sono protetti e sono proteggibili solo attraverso i meccanismo del web server) è utile introdurre una tipologia di risorsa nuova (LayerTMS) e, lato applicazioni, il relativo servizio.

1.4. Protezione accesso al FileSystem

Attualmente il File System condiviso è un volume del dispositivo di storage "NetApp" accessibile mediante protocollo Samba; la protezione di questa risorsa è basata sia sul binding dell'indirizzo IP che sugli utenti di dominio di Active Directory.
Sono stati creati anche alcuni utenti applicativi con sui sono lanciati i servizi Windows ArcIMS, Tomcat e Apache e a questi utenti sono stati assegnati privilegi opportuni su cartelle del volume condiviso.

1.5. Directory utenti unica

Un punto fondamentale dell'architettura di sicurezza che si vuole implementare è la costituzione di una directory utenti unica. Questa directory può essere "virtualmente" unica, nel senso che qualora tecnologicamente non si possa raggiungere tale risultato e si debbano replicare gli utenti, questo deve essere fattibile in maniera automatica mediante connettori che garantiscano la sincronizzazione. Il nodo cruciale da risolvere è l'unificazione delle directory di utenti di Oracle e del Domain Controller della rete Windows, che sono i principali repository di utenti del nostro sistema.

1.6. Sistema di controllo degli accessi nel SIT2COM

Il sistema utilizzato nel SIT2COM si basa fortemente sull'utilizzo di Active Directory e del Repertorio. E' stata creato un dominio AD isolato rispetto a "sitrs.regione.sardegna.net" che è "comuniras.net".

Le applicazioni desktop utilizzabili dagli utenti sfruttano l'autenticazione del repertorio nella configurazione particolare di "trust del dominio" ovvero esse sono configurate in modo da accettare l'autenticazione che il controllore di dominio windows effettua al login. Esse quindi non richiedono la password.

Ciascuna applicazione viene comunque attivata non direttamente, ma attraverso un'applicazione di lancio che ha la funzione di gestire l'auditing e recuperare l'ente precedentemente selezionato dall'utente tramite apposita utilità.

Sono state sviluppate due consolle per il provisioning: una dedicata all'amministratore regionale ed una a quello comunale. L'amministratore regionale crea solamente gli amministratori comunali e sono questi ultimi che hanno la responsabilità di creare gli utenti comunali e associare ad essi le relative autorizzazioni. Gli utenti creati dall'amministratore comunale hanno bisogno di un avvallo da parte di quello regionale che è l'unico che ha i diritti di inserire nuovi utenti nella AD.

Per Civilia, applicazione web per la gestione delle Pratiche Edilizie, c'è una replica della directory utenti gestita dalla console d amministrazione.

2. Censimento entità esistenti nella IDT

In questo capitolo vengono censite le **applicazioni**, i **servizi** ed i **dati** della IDT da considerarsi **risorse** da assoggettare al controllo degli accessi.
Vengono censite anche le **azioni** possibili sulle risorse individuate; esse vengono poi raggruppate in **policy** di autorizzazione.
Infine si definiscono i **profili** ovvero insiemi di policy di autorizzazione.

Come da indicazioni della Direzione Lavori il censimento contenuto nel presente documento è esaustivo solamente su alcune tipologie di oggetti. Vista infatti al natura statica di un documento testuale e la dinamicità con cui si definiscono nella IDT nuovi dati, nuovi servizi, ecc. si è preferito produrre unitamente a questo documento, un database in formato Microsoft Access con uno schema che implementa il modello concettuale di Figura 1.
Per ciascuna entità verrà specificata comunque la fonte da cui sono prelevate le informazioni.

2.1. Definizione modalità uniforme per identificazione entità trattate

Per poter effettuare un censimento significativo occorre prima di tutto scegliere una modalità di codifica chiara e uniforme. Qui sotto proponiamo di utilizzare una modalità stile "URN" (RFC 2141) che fornisce al contempo una chiave utilizzabile dalle macchine e leggibile per l'uomo.

```
<ID_SITR> ::= "urn:" <NID> ":" <NSS>

<NID> ::= "sitr"
<NSS> ::= "ENTITY" ":" <ID>

<ENTITY> ::= "res|act|pro"
<ID> ::= <string>


NID = Namespace Identifier
NSS = Namespace Specific String
```

I valori possibili di ENTITY hanno il seguente significato:

- res = risorsa
- act = azione
- pro = profilo

che rappresentano le tre grosse categorie di entità in ballo.

2.1.1. Risorse

Le risorse da sottoporre a controllo degli accessi si dividono in due grandi gruppi: **dati** e **applicazioni**.

Il **dato** può essere reso disponibile attraverso differenti interfacce e ciascuna di queste può essere considerata come diversa rappresentazione del dato stesso. Le diverse modalità di accesso ai dati, vista l'architettura della IDT del SITR, sono quindi:

- Tabella spaziale SDO
- Tabella spaziale ArcSDE
- File geografico raster
- Documento GML (WFS)
- Documento GML (WCS)
- Immagine georeferenziata (Layer WMS)
- Insieme di tasselli georeferenziati (Layer TMS)
- Contenuto di uno schema Oracle
- Cartella di File System

Le **applicazioni** invece le possiamo ulteriormente classificare, sempre a seconda dell'interfaccia che mostrano (in questo caso se è umana o applicativa) in:

- Applicazioni
- Servizi

2.1.1.1. Gruppi di risorse

Per semplificare la gestione delle autorizzazioni nel caso di elevata numerosità delle risorse di cui occorre controllare l'accesso e in situazioni di gestione omogenea delle policy è comodo introdurre il concetto di "**gruppo di risorse**".

Utilizziamo quindi il concetto di "dataset", "featurelist", "map" e "appset" per raggruppare rispettivamente:

- **dataset**: tabelle/viste Oracle e file geografici raster
- **dataset sde:**: tabelle/viste ArcSDE
- **featurelist**: feature type
- **map**: layer
- **appset**: applicazioni

2.1.1.2. Nomenclatura

Viste le premesse, per le risorse da sottoporre a controllo degli accessi si propongono le seguenti regole di nomenclatura per formulare quindi il NSS:

```
<NSS> ::= "res:" <TYPE> "-" <PROG> "-" <NAME>
<TYPE> ::= "app|srv|dts|dss|dbo|dbs|dir|sde|fso|lyr|map|ftc|ftl|aps|tml"
<PROG> ::= <literal>
<NAME> ::= <string>
```

I tipi di risorsa sono elencati nella tabella seguente:

ResourceType	Descrizione	urn
app	Applicazione	urn:sitr:rst:app
srv	Servizio	urn:sitr:rst:srv
dts	Dataset: gruppo di dati	urn:sitr:rst:dts
dss	Dataset sde: gruppo di dati	urn:sitr:rst:dss
dbo	Dato: Oggetto DB Oracle, vista o tabella	urn:sitr:rst:dbo
dbs	Schema DB: inteso solo come raggruppamento dei relative dbo	urn:sitr:rst:dbs
dir	Cartella di File System	urn:sitr:rst:dir
sde	Dato: Oggetto DB Oracle catalogato in SDE.	urn:sitr:rst:sde
fso	Dato: Oggetto File System, file	urn:sitr:rst:fso
lyr	Layer	urn:sitr:rst:lyr
map	Mappa: insieme di layer	urn:sitr:rst:map
ftc	Feature Type	urn:sitr:rst:ftc
ftl	Feature Type List: gruppo di Feature Type	urn:sitr:rst:ftl
aps	Application Set: gruppo di applicazioni	urn:sitr:rst:aps
tml	Layer TMS	urn:sitr:rst:tml

Tabella 1 - Tipi di risorse

2.2. Identificazione risorse: applicazioni

In questo paragrafo vengono censite le applicazioni che sono interessate dall'operazione di messa in sicurezza. Per un censimento più completo sono state rilevate anche le applicazioni non esattamente facenti parte della IDT, ma classificate come applicazioni verticali (sia di consultazione che di gestione) I dettagli di ciascuna di esse sono stati riportati nel documento "SITR-DB-024(C) - Elenco applicazioni" che è stato aggiornato appunto alla versione "C".

In questa occasione sono stati rivisti i nomi e codici utilizzati e sostituiti con quelli definiti in questo documento. Il foglio Excel è stato inoltre ulteriormente normalizzato al fine di poter utilizzare lo stesso per produrre il file XML con cui si alimenta un componente del Cruscotto IDT.

La fonte di questo elenco è eterogenea e si basa soprattutto sulla documentazione di progetto relativa alle varie attività di sviluppo.

Nome	Id	IDT
GestoreMetadati	urn:sitr:res:app-0001-GestoreMetadati	X
GestoreFeatureCatalogue	urn:sitr:res:app-0002-GestoreFeatureCatalogue	X
CatalogoDati	urn:sitr:res:app-0003-CatalogoDati	X
Geoserver-1	urn:sitr:res:app-0004-Geoserver-1	X
Tomcat6-1	urn:sitr:res:app-0005-Tomcat6-1	X
Tomcat6-2	urn:sitr:res:app-0006-Tomcat6-2	X
Tomcat6-3	urn:sitr:res:app-0007-Tomcat6-3	X
Tomcat5-1	urn:sitr:res:app-0008-Tomcat5-1	X
ArcIMS-Admin	urn:sitr:res:app-0009-ArcIMSAdmin	X
ArcIMS	urn:sitr:res:app-0010-ArcIMS	X
Jboss5-1	urn:sitr:res:app-0011-Jboss5-1	X
FeatureCatalogue	urn:sitr:res:app-0012-FeatureCatalogue	X
Oracle	urn:sitr:res:app-0013-Oracle	X
Apache-1	urn:sitr:res:app-0014-Apache-1	X
ActiveDirectorySITRS	urn:sitr:res:app-0015-ActiveDirectorySITRS	X
GeoWebCache-1	urn:sitr:res:app-0016-GeoWebCache-1	X
ArcSDE-1	urn:sitr:res:app-0017-ArcSDE-1	X
ArcSDE-2	urn:sitr:res:app-0018-ArcSDE-2	X
Sardegna2D	urn:sitr:res:app-0019-Sardegna2D	X
SardegnaMappe	urn:sitr:res:app-0020-SardegnaMappe	X
WMSConnector4	urn:sitr:res:app-0021-WMSConnector4	X
WMSConnector9	urn:sitr:res:app-0022-WMSConnector9	X
RepositoryManager	urn:sitr:res:app-0023-RepositoryManager	X
FME	urn:sitr:res:app-0024-FME	X
ScaricoCartografia	urn:sitr:res:app-0025-ScaricoCartografia	X
ConversioneCRS	urn:sitr:res:app-0026-ConversioneCRS	X
Sardegna3D	urn:sitr:res:app-0027-Sardegna3D	X
MySQL	urn:sitr:res:app-0028-MySQL	
MySQLAdmin	urn:sitr:res:app-0029-MySQLAdmin	
WordPress	urn:sitr:res:app-0030-WordPress	
Apache-2	urn:sitr:res:app-0031-Apache-2	X
Apache-3	urn:sitr:res:app-0032-Apache-3	X
Jboss4-1	urn:sitr:res:app-0033-Jboss4-1	X
GestoreToponimi	urn:sitr:res:app-0034-GestoreToponimi	
GestoreAnagraficaPUC	urn:sitr:res:app-0035-GestoreAnagraficaPUC	
GestoreStruttureTuristiche	urn:sitr:res:app-0036-GestoreStruttureTuristiche	
GestoreStrutturePOI	urn:sitr:res:app-0037-GestoreStrutturePOI	
ConsRAS	urn:sitr:res:app-0038-ConsRAS	
VerificaCoerenza	urn:sitr:res:app-0039-VerificaCoerenza	

SistemaTrasmissione	urn:sitr:res:app-0040-SistemaTrasmissione	
GestioneAbusi	urn:sitr:res:app-0041-GestioneAbusi	
GeoBlog	urn:sitr:res:app-0042-GeoBlog	
ConsultazioneAnagrafePUC	urn:sitr:res:app-0043-ConsultazioneAnagrafePUC	
ConsultazioneZonizzazionePUC	urn:sitr:res:app-0044-ConsultazioneZonizzazionePUC	
FotoAereeVigilanzaEdilizia	urn:sitr:res:app-0045-FotoAereeVigilanzaEdilizia	
ImmaginiAereeTelerilevate	urn:sitr:res:app-0046-ImmaginiAereeTelerilevate	
ConsultazioneTavolePPR	urn:sitr:res:app-0047-ConsultazioneTavolePPR	
RicercaToponimi	urn:sitr:res:app-0048-RicercaToponimi	
AnalisiAttivitaEdilizia	urn:sitr:res:app-0049-AnalisiAttivitaEdilizia	
ApacheLoadBalancer-1	urn:sitr:res:app-0050-ApacheLB-1	X
ApacheLoadBalancer-2	urn:sitr:res:app-0051-ApacheLB-2	X
ApacheLoadBalancer-3	urn:sitr:res:app-0052-ApacheLB-3	X
TassellatoreVettoriale	urn:sitr:res:app-0053-TassellatoreVettoriale	
TassellatoreRaster	urn:sitr:res:app-0054-TassellatoreRaster	
Tomcat5Manager-1	urn:sitr:res:app-0055-Tomcat5Mgr-1	X
Tomcat6Manager-1	urn:sitr:res:app-0056-Tomcat6Mgr-1	X
Tomcat6Manager-2	urn:sitr:res:app-0057-Tomcat6Mgr-2	X
Tomcat6Manager-3	urn:sitr:res:app-0058-Tomcat6Mgr-3	X
OssPPR	urn:sitr:res:app-0059-OssPPR	
ETL-1	urn:sitr:res:app-0101-ETL-1	X
ETL-2	urn:sitr:res:app-0102-ETL-2	X
…….	…….	X
ETL-130	urn:sitr:res:app-0229-ETL-129	X

Tabella 2 - Elenco applicazioni

2.2.1. GestoreMetadati

L'applicazione mostra una sola azione e un solo profilo possibile. In origine essa, collegata al Repertorio, era predisposta per mostrare le seguenti azioni:

- md_h_main = accesso
- md_h_tab = gestione tabelle
- md_h_sog = gestione soggetti
- md_h_serv = gestione metadati servizi
- md_h_acq = gestione metadati acquisizioni
- md_h_can = editing canali
- md_h_meta = gestione metadati dataset
- md_h_pub = gestione metadati pubblicazioni
- md_h_qdu = quadri di unione
- md_b_pub = visualizzazione pubblicazioni
- md_b_acq = visualizzazione acquisizioni
- md_b_meta = visualizzazione metadati dataset
- md_b_serv = visualizzazione metadati servizi

Lo scollegamento dal Repertorio ha avuto come effetto collaterale la perdita della possibilità di gestire le singole azioni ed il loro insieme costituisce un'azione unica <accesso_applicazione>.

2.2.1.1. Interventi

INT1- Eliminare utente applicazione "metadati"
INT2- (provvisorio) Introdurre 2 utente applicativi temporanei (finché non si effettuano modifiche per utilizzo utenti personali): uno per lettura autenticazione e uno per gestione metadati. In alternativa introdurre un utente personale per la connessione allo schema "metadati": questo in ciascun file di configurazione delle diverse postazioni previste.
INT3- (non in questa fase): Autenticazione LDAP
INT4- (non in questa fase): Introdurre/utilizzo utenti personali.

NOTA: *una feature dell'applicazione (attivabile o disattivabile da configurazione) è quella di considerare affidabile l'autenticazione di Windows e di non chiedere all'utente le credenziali quando viene lanciata. In questa configurazione l'applicazione verifica solo che l'utente Windows sia nelle tabelle del repertorio e abbia le necessarie autorizzazioni, ma non chiese la password. Questa caratteristica non potrà più essere attivata quando l'applicazione utilizzerà gli utenti personali perché per la connessione Oracle è necessaria la password che l'applicazione non può leggere dal S.O.*

2.2.2. GestoreFeatureCatalogue

Il GestoreFeatureCatalogue è stato sviluppato volutamente con un meccanismo di gestione degli accessi grezzo con una directory utenti gestita su file di configurazione e un unico profilo implicito.

2.2.2.1. Interventi

- Spostamento dati su nuovo schema "FC"
- Creazione utente applicativo oracle 000-APP-0002-000 con privilegi adeguati su oggetti schema (Attenzione: il primo deploy dell'applicazione crea gli oggetti DB di cui ha bisogno, se essi non vengono trovati).
- Modifica documentazione applicazione (per inserire i privilegi da assegnare all'utente).
- Eliminazione utenti attuali da file di configurazione.
- Introduzione credenziali utenti personali abilitati in file di configurazione.

2.2.3. Tomcat

Esistono 4 istanze di Tomcat (2 nei map server e 2 negli application server). Map server e Application Server sono costituiti ciascuno da una batteria di 3 macchine, per cui complessivamente ci sono 12 processi Tomcat in esecuzione, ciascuno con i propri dati di configurazione (non sono clusterizzati).
Per le finalità del presente documento, considereremo quindi le 4 istanze come applicazioni separate.

Le applicazioni contenute in Tomcat hanno in generale la necessità di collegarsi ad un database, per cui normalmente nei file di configurazione di Tomcat sono mantenute le credenziali (utente e password) per realizzare tali connessioni

Di seguito alcune considerazioni sul problema di mantenere queste in chiaro sul File System:

- Se vengono mantenute criptate mediante algoritmi non reversibili, allora il database deve supportare connessioni attraverso password criptate; in tal maniera venire a conoscenza della password criptata è del tutto uguale che conoscere la password in chiaro, visto che sarà possibile stabilire la connessione anche con quella criptata.
- Se viene utilizzato un algoritmo di crittazione reversibile allora è necessario usare un keyfile cioè un contenitore di chiavi di crittazione, che di solito viene mantenuto su File Sytem; per accedere a questo keyfile è necessaria una passphrase, ma a questo punto la passphrase deve essere mantenuta da Tomcat nei suoi file di configurazione e siamo daccapo.

In generale, quindi, la maniera migliore per garantire la sicurezza delle connessioni DB gestite da Tomcat:

- Limitare al massimo i privilegi sul DB dell'utente utilizzato;
- Assicurare che i file di configurazione di Tomcat siano accessibili solo dall'utente che lancia Tomcat.

2.2.4. SDE

Attenzione: è meglio dare i grant agli oggetti attraverso i comandi SDE!!!!

Verificare:

- ruoli SDE,
- quali diritti trasferisce sugli oggetti del DB

→ Introdurre un tipo di accesso diverso: "diretto per client ESRI" che include "diretto per client Oracle", ma non viceversa.

The grant and revoke operations control access to feature classes (layers). The grant operation allows the owner of a feature class (layer) to provide either SELECT, INSERT, UPDATE, or DELETE privileges to other users or roles. The revoke operation allows the owner to rescind previously granted privileges.

The following two commands grant and then revoke select privileges from user "bob".

```
$ sdelayer -o grant -l victoria,parcels -U bob -A SELECT -u av -p mo -i esri_80
$ sdelayer -o revoke -l victoria,parcels -U bob -A SELECT -u av -p mo -i esri_80
```

Granting privileges to roles is easier to maintain than repetitively granting the privileges to each user. Whenever possible create roles representing privileges that can be granted to a group of users.

2.2.5. Procedure ETL

Le procedure di ETL sono al momento 129. In generale infatti ogni ETL carica una sola FT. L'ambiente di authoring delle procedure (FME) è dotato di un'interfaccia visuale e non gestisce il controllo degli accessi. Un ETL fisicamente è un file testuale su file system che contiene istruzioni in un linguaggio di scripting proprietario della piattaforma (l'interprete è il "workbench FME"); può anche essere uno script Python che orchestra script FME o che può eseguire operazioni ausiliarie. Gli script Python in particolare gestisce l'autenticazione e la registrazione delle FT su SDE e la produzione dei pacchetti di scarico.
Le credenziali degli utenti sono scritti in un modulo Python comune a tutti gli ETL e sono quelli Oracle utilizzati per accedere ai DB operazionali, scrivere nel DBUnico e/o registrare le FT in SDE.

Gli ETL devono poter essere schedulati per cui non è possibile utilizzare utenti personali. I moduli Python in cui sono scritte le credenziali sono su file system condiviso le cui policy di accesso sono basate sia sul controllo degli IP (share su samba) e sia sugli utenti di domino AD.

Per quanto riguarda la messa in sicurezza, gli ETL possono essere considerati come le applicazioni server 3 tiers per cui è sufficiente considerare sicuro l'accesso ai file che memorizzano le credenziali.

Le procedure di ETL esistenti al momento sono contenute nella tabella sottostante. In questa tabella è evidenziata anche una possibile aggregazione degli ETL.

La fonte dell'elenco delle procedure di ETL sono i file "tbx" presenti nella cartella condivisa apposita del NetAPP.

Gruppo	File ETL
DB10K	DB10K/10K_ST04_idrografia.tbx
	DB10K/10K_ST05_altimetria.tbx
	DB10K/10K_ST07_reti_tecnologiche.tbx
	DB10K/10K_ST01_viabilita.tbx
	DB10K/10K_ST06_vegetazione.tbx
	DB10K/10K_ST10_aree_pertinenza.tbx
	DB10K/10K_ST09_limiti_amministrativi.tbx
	DB10K/10K_ST02_immobili.tbx
Catasto	Catasto/acqueCatasto.tbx
	Catasto/testiParticelleCatasto.tbx
	Catasto/fogliCatasto.tbx
	Catasto/testiCatasto.tbx
	Catasto/campitureCatasto.tbx
	Catasto/centroidiCatasto.tbx
	Catasto/simboliCatasto.tbx
	Catasto/puntiFiducialiCatasto.tbx
	Catasto/stradeCatasto.tbx

Gruppo	File ETL
	Catasto/particelleCatasto.tbx
cartaGeologica	cartaGeologica/autoriRevisioniGeologia.tbx
	cartaGeologica/geologiaLineari.tbx
	cartaGeologica/geologiaAreali.tbx
	cartaGeologica/geologiaPuntuali.tbx
	cartaGeologica/autoriRicercaGeomineràriaBase.tbx
	cartaGeologica/autoriCARG.tbx
POI	POI/poiSentieriEnteForeste.tbx
	POI/poiStruttureTuristiche.tbx
	POI/poiEnteForeste.tbx
	POI/poiGenerici.tbx
enteForeste	enteForeste/databaseOperazionale.tbx
	enteForeste/unitaGestionaliBase.tbx
	enteForeste/sentieri.tbx
quadriUnione	quadriUnione/quadroUnione50k.tbx
	quadriUnione/quadroUnione10k.tbx
	quadriUnione/quadroUnione25k.tbx
acquePubbliche	acquePubbliche/acquePubbliche.tbx
PPR	PPR/architSpecialistCiviliStoriche.tbx
	PPR/centraleElettrica.tbx
	PPR/zoneProtezioneSpeciale.tbx
	PPR/insediamentiArcheologici.tbx
	PPR/discariche.tbx
	PPR/grotteCaverne.tbx
	PPR/architettureReligiose.tbx
	PPR/lineaElettrica.tbx
	PPR/edificatoUrbanoCTR.tbx
	PPR/areeQuotaSuperiore900m.tbx
	PPR/areeFunerarie.tbx
	PPR/elemIndividuiStoricoArtistici.tbx
	PPR/areeEstrattiveCaveMiniere.tbx
	PPR/cicloRifiuti.tbx
	PPR/elementiIdrografici.tbx
	PPR/areeSpecialiAreeMilitari.tbx
	PPR/parchiAreeProtetteNazLqn394-91.tbx
	PPR/insediamentoStoricoSparso.tbx
	PPR/espansioniFinoAnni50.tbx
	PPR/areeGestSpecialeEnteForeste.tbx
	PPR/espansioniRecenti.tbx
	PPR/depuratori.tbx
	PPR/fasciaCostiera.tbx
	PPR/vincoli.tbx

Gruppo	File ETL
	PPR/areeInteresseFaunistico.tbx
	PPR/areeInteresseBotanicoFitogeogr.tbx
	PPR/areeInteressateImpiantiEolici.tbx
	PPR/areePreesisValenzaStoricoCult.tbx
	PPR/condottaIdrica.tbx
	PPR/sistemaRegParchiRiserveMonNat.tbx
	PPR/PPRelementiIdrici.tbx
	PPR/areeMinerarieDismesse.tbx
	PPR/insediamentiProduttivi.tbx
	PPR/scavi.tbx
	PPR/nodiTrasporti.tbx
	PPR/archeologieIndustrAreeEstrat.tbx
	PPR/ambitiPaesaggio.tbx
	PPR/edificatoUrbanoDiffuso.tbx
	PPR/impiantiFerroviariLineari.tbx
	PPR/areeSalineStoriche.tbx
	PPR/architettureMilitari.tbx
	PPR/parchiEolici.tbx
	PPR/edificatoUrbanoDiffusoCTR.tbx
	PPR/sistemiCostieri.tbx
	PPR/vulcani.tbx
	PPR/centriAnticaPrimaFormazione.tbx
	PPR/compPaesaggioValenzaAmbientale.tbx
	PPR/sitiInquinati.tbx
	PPR/nucleiCaseSparseInsediamSpec.tbx
	PPR/update/UPD_PPR_AI15_DEPURATORI.tbx
	PPR/update/UPD_PPR_AI13_CICLO_RIFIUTI.tbx
	PPR/update/UPD_IDT_PR01G_AMBITI.tbx
	PPR/update/UPD_STG_IDT_AMBITI.tbx
	PPR/parcoGeomAmbientaleStorico.tbx
	PPR/reteInfrastrutturaleStorica.tbx
	PPR/areeBonifica.tbx
	PPR/areeInfrastrutture.tbx
	PPR/dbOperazionale/IDT_PR72G_PERIM_AMBITI.tbx
	PPR/dbOperazionale/IDT_PR71G_LINEA_COSTA.tbx
	PPR/dbOperazionale/IDT_PR73G_ELEM_IDRICI.tbx
	PPR/monumentiNatIstituitiLr31-89.tbx
	PPR/nucleiCaseSparseInsedSpecCTR.tbx
	PPR/reteStradale.tbx
	PPR/sitiInteresseComunitario.tbx
	PPR/oasiPermanentiProtFaunistica.tbx
	PPR/areeOrganizzazioneMineraria.tbx

Gruppo	File ETL
	PPR/alberiMonumentali.tbx
	PPR/insediamentiTuristici.tbx
	PPR/luoghiCulto.tbx
	PPR/saline.tbx
fasceRispetto	fasceRispetto/fascia300m.tbx
	fasceRispetto/fascia3000m.tbx
usoSuolo	usoSuolo/usoSuolo2008.tbx
	usoSuolo/usoSuolo2003.tbx
ambitiAmministrativi	ambitiAmministrativi/centriUrbani1995.tbx
	ambitiAmministrativi/limitiAmministrComunali.tbx
	ambitiAmministrativi/asl.tbx
	ambitiAmministrativi/distrettiAsl.tbx
	ambitiAmministrativi/svilLineareCostieroComunale.tbx
	ambitiAmministrativi/limitiAmministrProvinciali.tbx
	ambitiAmministrativi/limiteAmministrRegionale.tbx
	ambitiAmministrativi/limitiAmministrProvinciali2001.tbx
CFVA	CFVA/areeIncendiateTipol2006.tbx
	CFVA/areeIncendiateTipol2005.tbx
	CFVA/areeIncendiatePerim2005.tbx
	CFVA/areeIncendiatePerim2007.tbx
	CFVA/areeIncendiatePerim2008.tbx
	CFVA/areeIncendiatePerim2006.tbx
	CFVA/areeIncendiateTipol2007.tbx
	CFVA/areeIncendiateTipol2008.tbx
protezioneCivile	protezioneCivile/zoneAllerta.tbx
lavoriPubblici	lavoriPubblici/piccoliInvasi.tbx
fotoAeree	fotoAeree/graficoVolo1987.tbx
	fotoAeree/graficoVolo1968.tbx

Tabella 3 - Elenco ETL

Per poter gestire adeguatamente le autorizzazioni sulle procedure ETL è conveniente, come già anticipato, utilizzare i gruppi di applicazioni come risorsa su cui poter definire delle policy.

I gruppi di applicazioni sono stati definiti soprattutto per le procedure di ETL, molto numerose. Il raggruppamento è stato fatto sulla base delle cartelle in cui sono raggruppate le ETL, che corrispondono a dati omogenei per fonte o altre caratteristiche simili. In più sono stati introdotti i gruppi relativi a middleware funzionalmente analogo (Tomcat, Jboss, Apache) di cui sono presenti più istanze nella IDT e quelli del middleware geografico.

Gruppi	Codice
DB10K	urn:sitr:res:aps-0001-ETL-DB10K
Catasto	urn:sitr:res:aps-0002-ETL-Catasto
cartaGeologica	urn:sitr:res:aps-0003-ETL-CartaGeologica
POI	urn:sitr:res:aps-0004-ETL-POI
enteForeste	urn:sitr:res:aps-0005-ETL-EnteForeste

Gruppi	Codice
quadriUnione	urn:sitr:res:aps-0006-ETL-QuadriUnione
acquePubbliche	urn:sitr:res:aps-0007-ETL-AcquePubbliche
PPR	urn:sitr:res:aps-0008-ETL-PPR
fasce Rispetto	urn:sitr:res:aps-0009-ETL-FasceRispetto
uso Suolo	urn:sitr:res:aps-0010-ETL-UsoSuolo
ambitiAmministrativi	urn:sitr:res:aps-0011-ETL-AmbitiAmministrativi
CFVA	urn:sitr:res:aps-0012-ETL-CFVA
protezione Civile	urn:sitr:res:aps-0013-ETL-ProtezioneCivile
lavori Pubblici	urn:sitr:res:aps-0014-ETL-LavoriPubblici
foto Aeree	urn:sitr:res:aps-0015-ETL-FotoAeree
Tomcat	urn:sitr:res:aps-0101-MW-Tomcat
Jboss	urn:sitr:res:aps-0102-MW-JBOSS
Apache LB	urn:sitr:res:aps-0103-MW-Apache
WMSConnector	urn:sitr:res:aps-0104-GMW-WMSConnector
Geoserver	urn:sitr:res:aps-0105-GMW-Geoserver

Tabella 4 - Elenco delle "appset"

2.3. Identificazione risorse: servizi

Anche per i servizi la fonte da considerarsi è la documentazione di progetto delle attività di sviluppo.

Nome	Codice
WMS1Geoserver1	urn:sitr:res:srv-0001-WMS-1
WMS1ArcIMS	urn:sitr:res:srv-0002-WMS-1
WMS2ArcIMS	urn:sitr:res:srv-0003-WMS-2
WFS1Geoserver1	urn:sitr:res:srv-0004-WFS-1
WCS1Geoserver1	urn:sitr:res:srv-0005-WCS-1
ServiRepeSicurezza	urn:sitr:res:srv-0006-ServiRepeSicurezza
ServiRepeCatalogo	urn:sitr:res:srv-0007-ServiRepeCatalogo
ServiRepeDati	urn:sitr:res:srv-0008-ServiRepeDati
MetadatiISO	urn:sitr:res:srv-0009-MetadatiISO
Routing	urn:sitr:res:srv-0010-Routing
Geocoding	urn:sitr:res:srv-0011-Geocoding
RicercaToponimi	urn:sitr:res:srv-0012-RicercaToponimi
RicercaPOI	urn:sitr:res:srv-0013-RicercaPOI
ConsultazionePUC	urn:sitr:res:srv-0014-ConsultazionePUC
ConversioneCRS	urn:sitr:res:srv-0015-ConversioneCRS
ReverseGeocoding	urn:sitr:res:srv-0016-ReverseGeocoding
RoutingAccessibile	urn:sitr:res:srv-0017-RoutingAccessibile
SLDManager	urn:sitr:res:srv-0018-SLDManager
RicercaStruttureTuristiche	urn:sitr:res:srv-0019-RicercaStruttureTuristiche
XMLMarker	urn:sitr:res:srv-0020-RojaXMLMarker
GeoRSS	urn:sitr:res:srv-0021-RojaGeoRSS
S3D	urn:sitr:res:srv-0022-RojaS3D
Directory	urn:sitr:res:srv-0023-RojaDirectory
RicercaComune	urn:sitr:res:srv-0024-RojaRicercaComune
GestionePUC	urn:sitr:res:srv-0025-GestionePUC
TMS1	urn:sitr:res:app-0026-TMS1
TMS2	urn:sitr:res:app-0027-TMS2

Tabella 5 - Elenco Servizi

2.3.1. WMS1ArcIMS – WMS2ArcIMS

I servizi attivi sono:

- **fotocoste** (visualizza i fotogrammi per l'applicazione `FotoAereeVigilanzaEdilizia`)
- **ras_wms** (WMS dati raster del DB Unico)

- **rastavoleppr_wms** (visualizza mappe dei quadri di unione per applicazione `ConsultazioneTavolePPR`)
- **roja** (per esempi API Roja che interfacciano direttamente servizi ArcIMS)
- **sit_01_PUC** (consultazione mosaico zonizzazione in Sardegna2D tramite applicazione `ConsultazioneZonizzazionePUC`)
- **sit_01_dbtopo** (mappa DB Topografico Sardegna2D)
- **sit_01_ppr** (mappa PPR Sardegna2D
- **sit_01_topoweb** (consultazione toponimi attraverso l'applicazione `RicercaToponimi`)
- **sit_01_web** (mappa generica Sardegna2D)
- **sit_adm_01_fotocoste** (visualizza grafici di volo per l'applicazione `FotoAereeVigilanzaEdilizia`)
- **sitr_monitoraggio** (produzione tematismi con "torte" per applicazione `AnalisiAttivitaEdilizia`)

2.3.1.1. Interventi

I servizi seguenti possono essere spenti dopo avere migrato le applicazioni che li utilizzano agli analoghi servizi e dati relativi esposti da Geoserver:

- **fotocoste**: migrazione a nuova applicazione `FotoAereeVigilanzaEdilizia`
- **sit_adm_01_fotocoste**: migrazione a nuova applicazione `FotoAereeVigilanzaEdilizia`
- **rastavoleppr_wms**
- **sitr_monitoraggio**[1]

I servizi seguenti possono essere spenti senza migrazione alcuna:

- **sit_01_PUC**[2] (il mosaico è ormai datato e non omogeneo)

I servizi seguenti possono essere mantenuti previo aggiornamento della fonte dati che attualmente non punta ai dati del DBUnico.

- **sit_01_dbtopo** [3]
- **sit_01_ppr**[4]
- **sit_01_web**[5]

2.4. Identificazione risorse: schemi DB

Schema e utente sono due concetti coincidenti in Oracle (a meno di non utilizzare la feature "global authentication" con cui si possono definire utenti in una directory esterna –OID- che condividono uno

[1] Ora con Geoserver è possibile ottenere le stesse simbologie.
[2] Alla data odierna (19 Aprile 2010) il servizio è stato bloccato.
[3] Alla data odierna (19 Aprile 2010) la fonte dati risulta migrata.
[4] Idem
[5] Idem

stesso schema): qui consideriamo solo quegli schemi che contengono dati al loro interno e non quelli creati solo per utilizzare l'utente relativo per connettersi al DB.

2.4.1. Schemi attuali

Schema	Descrizione
IDT	Dati del DB Unico e Feature Catalogue
METADATI	Metadati dati e servizi
SDE	Catalogo metadati ArcSDE (istanza SITRS)
SIT_ADM	Ex-Dati db unico. Repertorio metadati applicativi.
SDE2	Catalogo metadati ArcSDE (secondo catalogo nell'istanza SITRS per test conpresenza cataloghi)
RASTURISMO	Applicazione di gestione delle strutture turistiche
RASPOI	Applicazione di gestione dei POI
CIVILIA	Verifica di coerenza PUC

Tabella 6 - Schemi DB attuali

2.4.2. Schemi futuri

Schema	Id	Descrizione
IDT	urn:sitr:res:dbs:0001-idt	Dati del DB Unico
IDT_MD	urn:sitr:res:dbs:0002-md	Metadati dati e servizi
SDE	urn:sitr:res:dbs:0003-sde	Catalogo metadati ArcSDE
SIT_ADM	urn:sitr:res:dbs:0004-sit	Repertorio metadati applicativi
IDT_FC	urn:sitr:res:dbs:0005-fc	FeatureCatalogue
ABEDI	urn:sitr:res:dbs:0006-ae	AbusiEdilizi
RASTURISMO	urn:sitr:res:dbs:0007-tur	Gestione Strutture Turistiche
RASPOI	urn:sitr:res:dbs:0008-poi	Gestione POI
TOPONIMI	urn:sitr:res:dbs:0009-topo	Gestione toponimi
ANAPUC	urn:sitr:res:dbs:0010-anapuc	Anagrafe PUC
INDEDI	urn:sitr:res:dbs:0011-indedi	Indicatori Attività Edilizia
CIVILIA	urn:sitr:res:dbs:0012-civ	Verifica coerenza
PPR	urn:sitr:res:dbs:0013-ppr	PPR

Tabella 7 - Schemi DB futuri

2.4.3. TMS

Da notare che il servizio di fatto non è implementato da nessun programma, ma coincide con la richiesta a risorse statiche servite dal web server. Nell'architettura della IDT esso è comunque modellato come un servizio (i dati su cui si appoggia possono venir considerati alla stregua di dati temporanei di un'applicazione).

2.5. Identificazione risorse: cartelle File System

In questo capitolo si prenderanno in considerazione, in termini di risorse da proteggere, solo le cartelle condivise, cioè disponibili per tutte le applicazioni server e desktop, posizionate su un apposito dispositivo.
Tale dispositivo è un volume del NetApp esposto con il protocollo Samba con il nome:

\\X.X.X.X\sitr_app_smb[6]

Tale volume è stato integrato al dominio SITRS ed è configurabile con policy di protezione che si basano sia sull'IP di provenienza delle richieste che sul utente di dominio che le formula.

In particolare al momento è stata predisposta una policy che filtra le richieste alle sole risorse poste nelle sottoreti:

- A.A.A.A – B.B.B.B – C.C.C.C (rete SITR)
- D.D.D.D – E.E.E.E (rete UFFICIOPIANO)

Le cartelle presenti sul volume sono elencate nella Tabella 8:

nome cartella	Contenuto	codice
ArcIMS	File AXL di configurazione servizi ArcIMS e immagini create dai servizi.	urn:sitr:res:dir:0001-arcims
BackupApp01	Backup del application server sitr-app-01	urn:sitr:res:dir:0002-buapp1
BackupApp02	Backup del application server sitr-app-02	urn:sitr:res:dir:0003-buapp2
BackupApp03	Backup del application server sitr-app-03	urn:sitr:res:dir:0004-buapp3
BackupGeoserver	Backup dei file di configurazione di Geoserver	urn:sitr:res:dir:0005-bugeos
BackupMap01	Backup del application server sitr-map-01	urn:sitr:res:dir:0006-bumap1
BackupMap02	Backup del application server sitr-map-02	urn:sitr:res:dir:0007-bumap2
BackupMap03	Backup del application server sitr-map-03	urn:sitr:res:dir:0008-bumap3
civiliaweb		urn:sitr:res:dir:0009-civilia
dati	dati raster del DB Unico	urn:sitr:res:dir:0010-dati
ETL	Procedure ETL di alimentazione DB Unico.	urn:sitr:res:dir:0011-ETL
geoblog	Contenuto multimediale in upload da parte degli utenti del GeoBlog	urn:sitr:res:dir:0012-geoblog
geoserver_data_dir	File di catalogo dei geoserver.	urn:sitr:res:dir:0013-geoscat
geowebcache	Cache dei tasselli WMS-C	urn:sitr:res:dir:0014-gwc
grigliati_igm	Grigliati IGM per la conversione di coordinate	urn:sitr:res:dir:0015-igm
scaricocartografia	Pacchetti di scarico preconfezionati	urn:sitr:res:dir:0016-scarico
temp_scarico	file temporanei applicazione di scarico online	urn:sitr:res:dir:0017-scartmp
TMS	Tasselli TMS[7]	urn:sitr:res:dir:0018-tms
DB_Operazionale	DB operazionali di gestione feature type	urn:sitr:res:dir:0019-dboper

Tabella 8 - Elenco cartelle condivise

Su tali risorse sono al momento assegnati questi permessi:

[6] E' in programma un'attività di passaggio da Samba a protocollo NFS.
[7] al momento, sebbene fisicamente sul NETAPP, la cartella non è condivisa ed è come se fosse locale ai web server che la utilizzano. Questo per problemi di performance con il software di condivisione (samba).

codice	policy
urn:sitr:res:dir:0001-arcims	apache: lettura/esecuzione arcims: full control siacovella: full control
urn:sitr:res:dir:0002-buapp1	(domains admins): full control
urn:sitr:res:dir:0003-buapp2	(domains admins): full control
urn:sitr:res:dir:0004-buapp3	(domains admins): full control
urn:sitr:res:dir:0005-bugeos	(domains admins): full control
urn:sitr:res:dir:0006-bumap1	(domains admins): full control
urn:sitr:res:dir:0007-bumap2	(domains admins): full control
urn:sitr:res:dir:0008-bumap3	(domains admins): full control
urn:sitr:res:dir:0009-civilia	siacovella: full control
urn:sitr:res:dir:0010-dati	tomcat6: full control arcims: full control
urn:sitr:res:dir:0011-ETL	adminlab1: full control siacovella: full control
urn:sitr:res:dir:0012-geoblog	apache: full control
urn:sitr:res:dir:0013-geoscat	tomcat6: full control siacovella: full control
urn:sitr:res:dir:0014-gwc	tomcat6: full control
urn:sitr:res:dir:0015-igm	adminlab1: lettura/esecuzione siacovella: full control
urn:sitr:res:dir:0016-scarico	apache: lettura/esecuzione siacovella: full control
urn:sitr:res:dir:0017-scartmp	tomcat6: full control apache: lettura/esecuzione

Tabella 9 - Privilegi su cartelle condivise

Oltre alle risorse presenti sul dispositivo di storage, ci sono quelle locali sui diversi server che elenchiamo nella tabella seguente, con i relativi permessi assegnati agli utenti:

cartella[8]	dominio	utente/gruppo[9]	permesso
sitrs3012 X.X.X.X backup server			
VM	SITRS	xxxxxxxx	READ
	SITRS	repository	READ
	UFFICIOPIANO	xxxxxxxx	READ
OrtofotoIT2006_ECW	UFFICIOPIANO	xxxxxxxx	READ
	UFFICIOPIANO	xxxxxxxx	READ
	SITRS	Laboratorio	READ
BackupSitrASMS	SITRS	patrol	FULL CONTROL
LinuxSitrs$	SITRS	patrol	FULL CONTROL
LinuxSitrsde$	SITRS	patrol	FULL CONTROL
Scanner		Everyone[10]	READ
	SITRS	Laboratorio	CHANGE
	SITRS	scanner	CHANGE

[8] Le cartelle che terminano in $ sono condivisioni nascoste.
[9] I gruppi, sia i built-in che quelli creati appositamente, hanno l'iniziale maiuscola.
[10] Gruppo virtuale, significa tutti, sia utenti locali che di dominio

cartella[8]	dominio	utente/gruppo[9]	permesso
	UFFICIOPIANO	xxxxxxxx	CHANGE
	UFFICIOPIANO	xxxxxxxx	CHANGE
BackupAlfresco	SITRS	patrol	FULL CONTROL
Repository	SITRS	repository	FULL CONTROL
tiles		Everyone	FULL CONTROL
Foto aeree 2k	SITRS	xxxxxxxx	FULL CONTROL
	SITRS3012	Administrator	READ
BackupSitrASMS	SITRS	patrol	FULL CONTROL
C		Everyone	READ
D		Everyone	READ
H		Everyone	READ
F		Everyone	READ
G		Everyone	READ
BackupOracleCluster$		Everyone	FULL CONTROL
Geowebcache_temp		Everyone	CHANGE
	SITRS3012	sviluppo	FULL CONTROL
download		Everyone	READ
BackupComuniras	SITRS	patrol	FULL CONTROL
Software		NT AUTHORITY/ Authenticated Users	READ
condivisa		Everyone	FULL CONTROL
backup_symantec		Everyone	READ
Workinprogress_SITR	SITRS3012	LaboratorioSITR	CHANGE
dump	SITRS3012	Administrator	READ
geowebcache_temp7		Everyone	CHANGE
	SITRS3012	sviluppo	FULL CONTROL
dc2sitrs X.X.X.X backup domain controller			
print$		Everyone	READ
	SITRS	Administrators	FULL CONTROL
	SITRS	Print Operators	FULL CONTROL
	SITRS	Server Operators	FULL CONTROL
cd		Everyone	READ
BackupGiornaliero$		Everyone	FULL CONTROL
hpdesign110		Everyone	FULL CONTROL
	SITRS	Administrators	FULL CONTROL
	SITRS	Print Operators	FULL CONTROL
	SITRS	Server Operators	FULL CONTROL
cdrom	SITRS	Administrators	FULL CONTROL
	SITRS	Users	READ
prnproc$		Everyone	READ
	SITRS	Administrators	FULL CONTROL
	SITRS	Print Operators	FULL CONTROL
	SITRS	Server Operators	FULL CONTROL
CITRIX	SITRS	xxxxxxxx	FULL CONTROL
License	SITRS	adminlab4	READ
	UFFICIOPIANO	xxxxxxxx	READ

cartella[8]	dominio	utente/gruppo[9]	permesso
sitr-app-02 X.X.X.X application server 2			
geoblog	SITRS	xxxxxxxx	FULL CONTROL
sitr-map-01 X.X.X.X map server 1			
ArcGIS 9.3 Desktop	SITRS	Domain Users	READ
		Everyone	READ
sitr4004 X.X.X.X web server			
C		Everyone	READ
F		Everyone	READ
E		Everyone	READ
nlb		Everyone	READ
TILES2003NUOVI		Everyone	FULL CONTROL
sitr4005 X.X.X.X web server			
C		Everyone	READ
F		Everyone	READ
E		Everyone	READ
nlb		Everyone	READ

Tabella 10 - Privilegi su cartelle su altri server

2.6. Identificazione risorse: dati

In questo capitolo l'elenco dei dati geografici attualmente nella IDT e quindi potenzialmente da proteggere.

2.6.1. Dati

I dati vettoriali della IDT sono costituiti tutti da tabelle spaziali contenute nello schema IDT della istanza SITR. Quelli raster sono al momento mantenuti su file system (volume Samba condiviso) in formato ECW. Di sotto l'elenco dei dati dove il "tipo" indica la natura vettoriale "V" o raster "R" del dato stesso.
La colonna "gruppo" presente nella Tabella 11 rappresenta il raggruppamento derivante dagli ETL di caricamento.

La fonte dell'elenco di Tabella 11 sono le tabelle o le viste Oracle presenti nello schema IDT e catalogate come oggetti spaziali nei metadati SDO. A questi si aggiungono i file raster contenuti nell'apposita cartella condivisa. Nella tabella non sono stati riportati volutamente tutti i codici delle risorse.

Gruppo	Nome tabella / file	Tipo	Codice

Gruppo	Nome tabella / file	Tipo	Codice
DBT10K	DBTSEDETRASPORTOFERRO	V	urn:sitr:res:dbo-0001-DBTSEDETRASPORTOFERRO
	DBTACQUEDOTTO	V	urn:sitr:res:dbo-0002-DBTACQUEDOTTO
	DBTALBEROISOLATO	V	urn:sitr:res:dbo-0003-DBTALBEROISOLATO
	DBTALVEOINCISO	V	urn:sitr:res:dbo-0004-DBTALVEOINCISO
	DBTALVEOINCISOARCHI	V	urn:sitr:res:dbo-0005-DBTALVEOINCISOARCHI
	DBTAREASERAEREOPORTUALE	V	urn:sitr:res:dbo-0006- DBTAREASERAEREOPORTUALE
	DBTAREASERAEREOPORTUALEPUNTI	V	urn:sitr:res:dbo-0007- DBTAREASERAEREOPORTUALEPUNTI
	DBTAREASERPORTUALE	V	urn:sitr:res:dbo-0008-DBTAREASERPORTUALE
	DBTAREASERPORTUALEPUNTI	V	9
	DBTAREASERSTRADALE	V	10
	DBTAREASERSTRADALEPUNTI	V	11
	DBTAREASERTRASPORTOFERRO	V	12
	DBTAREASERTRASPORTOFERROPUNTI	V	13
	DBTAREASTRADALE	V	14
	DBTAREASTRADALEARCHI	V	15
	DBTAREEALBERIARCHI	V	16
	DBTAREESERIMPINDUSTRIALI	V	17
	DBTAREESERIMPSTRUTTURE	V	18
	DBTAREEVERDI	V	19
	DBTBINARIOINDUSTRIALE	V	urn:sitr:res:dbo-0020-DBTBINARIOINDUSTRIALE
	DBTBOSCO	V	21
	DBTCOLTUREAGRICOLE	V	22
	DBTCOMUNE	V	23
	DBTCONDOTTA	V	24
	DBTCURVELIVELLO	V	25
	DBTDIGA	V	26
	DBTEDIFICIOEDILIZIA	V	27
	DBTELEMENTOALTROTRASPORTO	V	28
	DBTELEMENTOFERROVIARIO	V	29
	DBTELEMENTOIDRICO	V	30
	DBTELEMENTOSTRADALE	V	31
	DBTELEMENTOTRASPORTOFUNE	V	32
	DBTELETTRODOTTO	V	33
	DBTEMERGENZANATURALEACQUA	V	34
	DBTFORMAZIONIPARTICOLARI	V	35
	DBTFORMEARTIFICIALITERRENO	V	36
	DBTFORMENATURALITERRENOARCHI	V	37
	DBTGALLERIA	V	38
	DBTGIUNZIONEFERROVIARIA	V	39
	DBTGIUNZIONESTRADALE	V	40
	DBTINVASOARTIFICIALE	V	41
	DBTLINEACOSTAMARINA	V	42
	DBTMANUFATTIAEROPORTUALI	V	43
	DBTMANUFATTIAEROPORTUALIPUNTI	V	44
	DBTMANUFATTICULTO	V	45
	DBTMANUFATTIEDILIZI	V	46
	DBTMANUFATTIEDILIZIARCHI	V	47
	DBTMANUFATTIEDILIZIPUNTI	V	48
	DBTMANUFATTIIMPSPORTIVI	V	49
	DBTMANUFATTIIMPSPORTIVIARCHI	V	urn:sitr:res:dbo-0050- DBTMANUFATTIIMPSPORTIVIARCHI
	DBTMANUFATTIINDUSTRIALI	V	51
	DBTMANUFATTIINDUSTRIALIARCHI	V	52
	DBTMANUFATTIINDUSTRIALIPUNTI	V	53
	DBTMANUFATTIPORTUALI	V	54
	DBTMANUFATTIPORTUALIARCHI	V	55
	DBTMANUFATTIPORTUALIPUNTI	V	56
	DBTMANUFATTISTRADALI	V	57
	DBTMANUFATTISTRADALIARCHI	V	58
	DBTMETANODOTTO	V	59
	DBTMURIRECINZIONIDIVISIONI	V	urn:sitr:res:dbo-0060- DBTMURIRECINZIONIDIVISIONI
	DBTNODOIDRICO	V	61
	DBTOLEODOTTO	V	62

Gruppo	Nome tabella / file	Tipo	Codice
	DBTOPEREREGIMAZIONEIDRAULICA	V	63
	DBTPALIESOSTEGNI	V	64
	DBTPASCOLI	V	65
	DBTPILONEINPROTELETTRODOTTO	V	66
	DBTPONTEVIADOTTO	V	67
	DBTPONTEVIADOTTOARCHI	V	68
	DBTPRESAACQUEDOTTO	V	69
	DBTPROVINCIA	V	70
	DBTPUNTIPROIETTATISULGRAFO	V	71
	DBTPUNTIQUOTATI	V	72
	DBTREGIONE	V	73
	DBTSPECCHIOACQUA	V	urn:sitr:res:dbo-0074-DBTSPECCHIOACQUA
	DBTVIABILITAMISTASECONDARIA	V	75
	DBTVIABILITAMISTASECONDARCHI	V	76
PPR	ALBERIMONUMENTALI	V	77
	AMBITIPAESAGGIO	V	78
	ARCHEOLOGIEINDUSTRAREEESTRAT	V	79
	ARCHITSPECIALISTCIVILISTORICHE	V	80
	ARCHITETTUREMILITARI	V	81
	ARCHITETTURERELIGIOSE	V	82
	AREEBONIFICA	V	83
	AREEESTRATTIVECAVEMINIERE	V	84
	AREEFUNERARIE	V	85
	AREEGESTSPECIALEENTEFORESTE	V	86
	AREEINFRASTRUTTURE	V	87
	AREEINTERESSATEIMPIANTIEOLICI	V	88
	AREEINTERESSEBOTANICOFITOGEOGR	V	89
	AREEINTERESSEFAUNISTICO	V	urn:sitr:res:dbo-0090- AREEINTERESSEFAUNISTICO
	AREEMINERARIEDISMESSE	V	91
	AREEORGANIZZAZIONEMINERARIA	V	92
	AREEPREESISVALENZASTORICOCULT	V	93
	AREEQUOTASUPERIORE900M	V	94
	AREESALINESTORICHE	V	95
	AREESPECIALIAREEMILITARI	V	96
	CENTRALEELETTRICA	V	97
	CENTRIANTICAPRIMAFORMAZIONE	V	98
	CICLORIFIUTI	V	99
	COMPPAESAGGIOVALENZAAMBIENTALE	V	urn:sitr:res:dbo-0100-COMPPAESAGGIOVALENZAAMBIENTALE
	CONDOTTAIDRICA	V	
	DEPURATORI	V	
	DISCARICHE	V	
	EDIFICATOURBANOCTR	V	
	EDIFICATOURBANODIFFUSO	V	
	EDIFICATOURBANODIFFUSOCTR	V	
	ELEMINDIVIDUISTORICOARTISTICI	V	
	PPRELEMENTIIDRICI	V	
	ELEMENTIIDROGRAFICI	V	
	ESPANSIONIFINOANNI50	V	110
	ESPANSIONIRECENTI	V	
	GROTTECAVERNE	V	
	IMPIANTIFERROVIARILINEARI	V	
	INSEDIAMENTIARCHEOLOGICI	V	
	INSEDIAMENTIPRODUTTIVI	V	
	INSEDIAMENTITURISTICI	V	
	INSEDIAMENTOSTORICOSPARSO	V	
	LINEAELETTRICA	V	
	LUOGHICULTO	V	
	MONUMENTINATISTITUITILR31_89	V	120
	NODITRASPORTI	V	
	NUCLEICASESPARSEINSEDSPECCTR	V	
	NUCLEICASESPARSEINSEDIAMSPEC	V	

Gruppo	Nome tabella / file	Tipo	Codice
	OASIPERMANENTIPROTFAUNISTICA	V	
	RETEINFRASTRUTTURALESTORICA	V	
	RETESTRADALE	V	
	SALINE	V	
	SCAVI	V	
	SISTEMAREGPARCHIRISERVEMONNAT	V	
	SISTEMICOSTIERI	V	urn:sitr:res:dbo-0130-SISTEMICOSTIERI
	SITIINQUINATI	V	
	SITIINTERESSECOMUNITARIO	V	
	VINCOLI	V	
	VULCANI	V	
	ZONEPROTEZIONESPECIALE	V	
	ACQUEPUBBLICHE	V	
CFVA	AREEINCENDIATEPERIM2005	V	urn:sitr:res:dbo-137-AREEINCENDIATEPERIM2005
	AREEINCENDIATEPERIM2006	V	138
	AREEINCENDIATEPERIM2007	V	139
	AREEINCENDIATEPERIM2008	V	140
	AREEINCENDIATETIPOL2005	V	
	AREEINCENDIATETIPOL2006	V	
	AREEINCENDIATETIPOL2007	V	
	AREEINCENDIATETIPOL2008	V	
cartaGeologica	AUTORICARG	V	urn:sitr:res:dbo-0145-AUTORICARG
	AUTORIREVISIONIGEOLOGIA	V	
	GEOLOGIAAREALI	V	
	GEOLOGIALINEARI	V	
	GEOLOGIAPUNTUALI	V	
	AUTORIRICERCAGEOMINERARIABASE	V	urn:sitr:res:dbo-0150-AUTORIRICERCAGEOMINERARIABASE
ambitiAmministrativi	CENTRIURBANI1995	V	urn:sitr:res:dbo-0151-CENTRIURBANI1995
	ASL	V	
	DISTRETTIASL	V	
fasceRispetto	FASCIA3000M	V	urn:sitr:res:dbo-0153-FASCIA3000M
	FASCIA300M	V	
	FASCIACOSTIERA	V	
fotoAeree	GRAFICOVOLO1968	V	urn:sitr:res:dbo-0156-GRAFICOVOLO1968
	GRAFICOVOLO1987	V	
	INVILUPPIFOTOAEREE	V	
	LIMITEAMMINISTRREGIONALE	V	urn:sitr:res:dbo-0160-LIMITEAMMINISTRREGIONALE
	LIMITIAMMINISTRCOMUNALI	V	urn:sitr:res:dbo-0161-LIMITIAMMINISTRCOMUNALI
	LIMITIAMMINISTRPROVINCIALI	V	
	LIMITIAMMINISTRPROVINCIALI2001	V	
	PARCHIAREEPROTETTENAZLQN394_91	V	
	PARCOGEOMAMBIENTALESTORICO	V	
lavoriPubblici	PICCOLIINVASI	V	urn:sitr:res:dbo-0165-PICCOLIINVASI
enteForeste	POIENTEFORESTE	V	urn:sitr:res:dbo-0166-POIENTEFORESTE
POI	POIGENERICI	V	urn:sitr:res:dbo-0167-POIGENERICI
	POISENTIERIENTEFORESTE	V	
	POISTRUTTURETURISTICHE	V	urn:sitr:res:dbo-0170-POISTRUTTURETURISTICHE
quadriUnione	QUADROUNIONE10K	V	urn:sitr:res:dbo-0171-QUADROUNIONE10K
	QUADROUNIONE25K	V	
	QUADROUNIONE50K	V	
	SENTIERI	V	
	SVILLINEARECOSTIEROCOMUNALE	V	
	UNITAGESTIONALIBASE	V	
usoSuolo	USOSUOLO2003	V	urn:sitr:res:dbo-0177-USOSUOLO2003
	USOSUOLO2008	V	

Gruppo	Nome tabella / file	Tipo	Codice
	USOSUOLOCOLTURE2008	V	urn:sitr:res:dbo-0179-USOSUOLOCOLTURE2008
	USOSUOLOSTRATILINEARI2008	V	urn:sitr:res:dbo-0180- USOSUOLOSTRATILINEARI2008
protezioneCivile	ZONEALLERTA	V	urn:sitr:res:dbo-0181-ZONEALLERTA
catasto	ACQUECATASTO	V	urn:sitr:res:dbo-0182-ACQUECATASTO
	CAMPITURECATASTO	V	urn:sitr:res:dbo-0183-CAMPITURECATASTO
	CENTROIDICATASTO	V	urn:sitr:res:dbo-0184-CENTROIDICATASTO
	FOGLICATASTO	V	urn:sitr:res:dbo-0185-FOGLICATASTO
	PARTICELLECATASTO	V	urn:sitr:res:dbo-0186-PARTICELLECATASTO
	PUNTIFIDUCIALICASTASTO	V	urn:sitr:res:dbo-0187-PUNTIFIDUCIALICASTASTO
	SIMBOLICATASTO	V	urn:sitr:res:dbo-0188-SIMBOLICATASTO
	STRADECATASTO	V	urn:sitr:res:dbo-0189-STRADECATASTO
	TESTICATASTO	V	urn:sitr:res:dbo-0190-TESTICATASTO
	TESTIPARTICELLECATASTO	V	urn:sitr:res:dbo-0191-TESTIPARTICELLECATASTO
mosaici	ortofoto_it_2000	R	urn:sitr:res:fso-0001-ORTOFOTOIT2000
	ortofoto_it_2006	R	urn:sitr:res:fso-0002-ORTOFOTOIT2006
	Carta fisica	R	urn:sitr:res:fso-0003-CARTAFISICA
	CTR10K raster	R	urn:sitr:res:fso-0004-CTR10K

Tabella 11 - Elenco dati (oggetti DB e File System)

2.6.2. Dataset

I dataset (o gruppi di dati) al momento non esistono. Di seguito una ipotesi di raggruppamento dei dati con criteri sia di sicurezza sia basata sulla tipologia e genealogia del dato (si veda i raggruppamenti delle procedure di ETL).
L'introduzione dei dataset permette una semplificazione nella gestione delle policy: basta definire una policy su un dataset per farla ricadere su tutti i dati che lo compongono.
Un dataset può essere composto da "dbo" (come le Feature vettoriali) e "fso" (le Feature raster). La classificazione in dataset proposta non ha nulla a che vedere con quella derivante dai metadati, nel senso che in alcuni caso potrebbe coincidere, ma nella maggior parte potrebbe essere differente.

Dataset	codice
catasto	urn:sitr:res:dts-0001-Catasto
DB10K	urn:sitr:res:dts-0002-DB10K
cartaGeologica	urn:sitr:res:dts-0003-CartaGeologica
POI	urn:sitr:res:dts-0004-POI
enteForeste	urn:sitr:res:dts-0005-EnteForeste
quadriUnione	urn:sitr:res:dts-0006-QuadriUnione
acquePubbliche	urn:sitr:res:dts-0007-AcquePubbliche
PPR	urn:sitr:res:dts-0008-PPR
fasceRispetto	urn:sitr:res:dts-0009-FasceRispetto
usoSuolo	urn:sitr:res:dts-0010-UsoSuolo
ambitiAmministrativi	urn:sitr:res:dts-0011-AmbitiAmministrativi
CFVA	urn:sitr:res:dts-0012-CFVA
protezioneCivile	urn:sitr:res:dts-0013-ProtezioneCivile
lavoriPubblici	urn:sitr:res:dts-0014-LavoriPubblici
fotoAeree	urn:sitr:res:dts-0015-FotoAeree

Tabella 12 - Elenco DataSet

2.6.3. Layer

L'elenco dei layer è derivato dalla GetCapabilities dei servizi WMS esposti dalla IDT.

layer	Codice
dbu:DBTSEDETRASPORTOFERRO	urn:sitr:res:lyr-0001-DBTSEDETRASPORTOFERRO
dbu:DBTACQUEDOTTO	urn:sitr:res:lyr-0002-DBTACQUEDOTTO
dbu:DBTALBEROISOLATO	urn:sitr:res:lyr-0003-DBTALBEROISOLATO
dbu:DBTALVEOINCISO	urn:sitr:res:lyr-0004-DBTALVEOINCISO
dbu:DBTALVEOINCISOARCHI	urn:sitr:res:lyr-0005-DBTALVEOINCISOARCHI
dbu:DBTAREASERAEREOPORTUALE	urn:sitr:res:lyr-0006-DBTAREASERAEREOPORTUALE
dbu:DBTAREASERAEREOPORTUALEPUNTI	urn:sitr:res:lyr-0007-DBTAREASERAEREOPORTUALEPUNTI
dbu:DBTAREASERPORTUALE	urn:sitr:res:lyr-0009-DBTAREASERPORTUALE
dbu:DBTAREASERPORTUALEPUNTI	urn:sitr:res:lyr-0010-DBTAREASERPORTUALEPUNTI
…	…
cat:TESTIPARTICELLECATASTO	urn:sitr:res:lyr-0191-TESTIPARTICELLECATASTO
ortofoto_it_2000	urn:sitr:res:lyr-1001-ortofoto_it_2000
ortofoto_it_2006	urn:sitr:res:lyr-1002-ortofoto_it_2006
Carta fisica	urn:sitr:res:lyr-1003-carta_fisica
CTR10K raster	urn:sitr:res:lyr-1004-CTR10K_raster

Tabella 13 - Elenco layer

2.6.4. Layer TMS

I layer TMS sono stati ricavati dalle applicazioni che al momento utilizzano tali dati: SardegnaMappe, FotoAeree e Sardegna3D.

TMS	layer TMS	formato	Codice
http://geowebcache.italia3d.it/	stradario_EPSG3003	png	urn:sitr:res:tml-0001-stradario_EPSG3003
http://geowebcache.italia3d.it/	ortofoto2006_EPSG3003	png	urn:sitr:res:tml-0002-ortofoto2006_EPSG3003
http://geowebcache.italia3d.it/	stradtrasp_EPSG3003	png	urn:sitr:res:tml-0003-stradtrasp_EPSG3003
http://webgis.regione.sardegna.it/tms/	ortofoto2003_EPSG3003	png	urn:sitr:res:tml-0004-ortofoto2003_EPSG3003
http://webgis.regione.sardegna.it/tms/	ortofoto2006_EPSG3003	jpg	urn:sitr:res:tml-0005-ortofoto2006_EPSG3003
http://webgis.regione.sardegna.it/tms/	ortofoto2000_EPSG3003	jpg	urn:sitr:res:tml-0006-ortofoto2000_EPSG3003
http://webgis.regione.sardegna.it/tms/	ortofoto1954_EPSG3003	png	urn:sitr:res:tml-0007-ortofoto1954_EPSG3003
http://geowebcache.italia3d.it/	tiles3Dstrade	png	urn:sitr:res:tml-0008- tiles3Dstrade

Tabella 14 - Elenco layer TMS

2.6.5. Gruppi di layer (Map)

I raggruppamenti di layer si possono fare coincidere con il namespace utilizzato in Geoserver integrato con il gruppo di layer esposti dal WMS ESRI. Nei gruppi di layer possono esserci anche gruppi di layer

TMS. Consideriamo come gruppi di layer anche i map service ArcIMS utilizzati per Sardegna2D e potenzialmente esponibili attraverso il servizio WMS offerto attraverso il ConnettoreWMS.

codice gruppo	layer
urn:sitr:res:map-0001-catasto	urn:sitr:res:lyr-0183-ACQUECATASTO
	. . .
	urn:sitr:res:lyr-0191-TESTIPARTICELLECATASTO
urn:sitr:res:map-0002-dbu	urn:sitr:res:lyr-0001-DBTSEDETRASPORTOFERRO
	. . .
	urn:sitr:res:lyr-0180-ZONEPROTEZIONESPECIALE
urn:sitr:res:map-0003-ortofoto	urn:sitr:res:lyr-1001-ortofoto_it_2000
	urn:sitr:res:lyr-1002-ortofoto_it_2006
urn:sitr:res:map-0004-tms1	urn:sitr:res:tml-0005-ortofoto2006_EPSG3003
urn:sitr:res:map-0005-tms2	urn:sitr:res:tml-0001-stradario_EPSG3003
urn:sitr:res:map-0006-tms3	urn:sitr:res:tml-0003-stradtrasp_EPSG3003
urn:sitr:res:map-0026-aims1	<layer esposti dal profile “web”>
urn:sitr:res:map-0027-aims2	<layer esposti dal profile “puc”>
urn:sitr:res:map-0028-aims3	<layer esposti dal profile “dbtopo”>
urn:sitr:res:map-0029-aims4	<layer esposti dal profile “ppr”>

Tabella 15 - Gruppi di layer

2.6.6. Tabelle SDE

Questo elenco di risorse è tratto dalla tabella di metadati SDE (tabella LAYERS), visualizzabile facilmente collegandosi con un client ArcGIS.

tabella	Codice
DBTSEDETRASPORTOFERRO	urn:sitr:res:sde-0001-DBTSEDETRASPORTOFERRO
DBTACQUEDOTTO	urn:sitr:res:sde-0002-DBTACQUEDOTTO
DBTALBEROISOLATO	urn:sitr:res:sde-0003-DBTALBEROISOLATO
DBTALVEOINCISO	urn:sitr:res:sde-0004-DBTALVEOINCISO
DBTALVEOINCISOARCHI	urn:sitr:res:sde-0005-DBTALVEOINCISOARCHI
DBTAREASERAEREOPORTUALE	urn:sitr:res:sde-0006-DBTAREASERAEREOPORTUALE
DBTAREASERAEREOPORTUALEPUNTI	urn:sitr:res:sde-0007-DBTAREASERAEREOPORTUALEPUNTI
DBTAREASERPORTUALE	urn:sitr:res:sde-0009-DBTAREASERPORTUALE
DBTAREASERPORTUALEPUNTI	urn:sitr:res:sde-0010-DBTAREASERPORTUALEPUNTI
…	…
TESTIPARTICELLECATASTO	urn:sitr:res:sde-0191-TESTIPARTICELLECATASTO

Tabella 16 - Elenco tabelle SDE

2.6.7. DataSet SDE

I dataset SDE sono stati definiti in maniera del tutto analoga a quella dei dataset di tabelle SDO.

Dataset	codice
catasto	urn:sitr:res:dss-0001-Catasto
DB10K	urn:sitr:res:dss-0002-DB10K
cartaGeologica	urn:sitr:res:dss-0003-CartaGeologica
POI	urn:sitr:res:dss-0004-POI
enteForeste	urn:sitr:res:dss-0005-EnteForeste
quadriUnione	urn:sitr:res:dss-0006-QuadriUnione
acquePubbliche	urn:sitr:res:dss-0007-AcquePubbliche
PPR	urn:sitr:res:dss-0008-PPR
fasceRispetto	urn:sitr:res:dss-0009-FasceRispetto
usoSuolo	urn:sitr:res:dss-0010-UsoSuolo
ambitiAmministrativi	urn:sitr:res:dss-0011-AmbitiAmministrativi
CFVA	urn:sitr:res:dss-0012-CFVA
protezioneCivile	urn:sitr:res:dss-0013-ProtezioneCivile
lavoriPubblici	urn:sitr:res:dss-0014-LavoriPubblici
fotoAeree	urn:sitr:res:dss-0015-FotoAeree

Tabella 17 - Elenco DataSet SDE

2.6.8. FeatureType

Questo elenco è derivato dalla GetCapabilities del servizio WFS integrato con le Feature Type raster (non ancora esposto da un servizio WCS).

Feature Type	Codice
dbu:DBTSEDETRASPORTOFERRO	urn:sitr:res:ftc-0001-DBTSEDETRASPORTOFERRO
dbu:DBTACQUEDOTTO	urn:sitr:res:ftc-0002-DBTACQUEDOTTO
dbu:DBTALBEROISOLATO	urn:sitr:res:ftc-0003-DBTALBEROISOLATO
dbu:DBTALVEOINCISO	urn:sitr:res:ftc-0004-DBTALVEOINCISO
dbu:DBTALVEOINCISOARCHI	urn:sitr:res:ftc-0005-DBTALVEOINCISOARCHI
dbu:DBTAREASERAEREOPORTUALE	urn:sitr:res:ftc-0006-DBTAREASERAEREOPORTUALE
dbu:DBTAREASERAEREOPORTUALEPUNTI	urn:sitr:res:ftc-0007-DBTAREASERAEREOPORTUALEPUNTI
dbu:DBTAREASERPORTUALE	urn:sitr:res:ftc-0009-DBTAREASERPORTUALE
dbu:DBTAREASERPORTUALEPUNTI	urn:sitr:res:ftc-0010-DBTAREASERPORTUALEPUNTI
. . .	. . .
dbu:DBTSPECCHIOACQUA	urn:sitr:res:ftc-0074-DBTSPECCHIOACQUA
. . .	. . .
dbu:CENTRIURBANI1995	urn:sitr:res:ftc-0151-CENTRIURBANI1995
. . .	. . .
cat:TESTIPARTICELLECATASTO	urn:sitr:res:ftc-0191-TESTIPARTICELLECATASTO
ortofoto_it_2000	urn:sitr:res:ftc-1001-ortofoto_it_2000
ortofoto_it_2006	urn:sitr:res:ftc-1002-ortofoto_it_2006
Carta fisica	urn:sitr:res:ftc-1003-carta_fisica
CTR10K raster	urn:sitr:res:ftc-1004-CTR10K_raster

Tabella 18 - Elenco Feature Type

2.6.9. Gruppi di FeatureType

I gruppo di feature type sono definiti a partire da considerazioni sulle limitazioni di accesso: esiste quindi un gruppo "catasto" che deve essere protetto e tutte le altre FT sono state raggruppate in un unico gruppo "dbu".

codice gruppo	feature type
urn:sitr:res:ftl-0001-catasto	urn:sitr:res:ftc-0182-ACQUECATASTO
	. . .
	urn:sitr:res:ftc-0191-TESTIPARTICELLECATASTO
urn:sitr:res:ftl-0002-dbu	urn:sitr:res:ftc-0001-DBTSEDETRASPORTOFERRO
	. . .
	urn:sitr:res:ftc-0181-ZONEPROTEZIONESPECIALE

Tabella 19 - Elenco gruppi feature type

2.7. Identificazione utenti

In questo capitolo verranno censiti utenti, domini ed azioni attualmente presenti nella IDT.

2.7.1. Domini attuali

Gli attuali domini presenti nel SITR sono svariati e sono elencati nella Tabella 20

dominio	tipo
GestoreFeatureCatalogue	locale su file (applicazione)
GestoreMetadati	locale su tabelle DB (applicazione)
Geoserver	locale su file (Middleware GIS)
ActiveDirectory SITRS	Dominio di rete WINDOWS "SITRS"
ActiveDirectory UFFICIOPIANO	Dominio di rete WINDOWS "UFFICIOPIANO"
Oracle	DBMS
Repertorio	centralizzato su DB (directory proprietaria)
Tomcat	locale (Middleware)
ArcIMS	locale su file (Middleware GIS)
AbusiEdilizi	locale (applicazione)
GestoreStruttureTuristiche	locale su tabelle DB (applicazione)
GeoBlog	locale su tabelle DB mySQL

Tabella 20 - Domini esistenti

I principali repository sono, nell'ordine, i seguenti 3:

- Active Directory (sia SITR che UFFICIOPIANO; i domini sono trusted)
- Oracle

- Repertorio

2.7.2. Utenti attuali

Gli utenti sono prelevati dai domini elencati nella Tabella 20.

utente	dominio	gruppo/ruolo
fcuser1 fcuser2	GestoreFeatureCatalogue	*<ruolo unico>*
metadati	GestoreMetadati	*<ruolo unico>*
xxxxxxxx xxxxxxxx xxxxxxxx	Geoserver	ROLE_CATASTO
admin	Geoserver	ROLE_ADMINISTRATOR (predefinito)
(utenti non listati)	ActiveDirectoryUFFICIOPIANO	
adminlab5 adminlab6 xxxxxxxx apache arcims xxxxxxxx xxxxxxxx xxxxxxxx backupuffpiano core xxxxxxxx etl geoview xxxxxxxx xxxxxxxx xxxxxxxx middleaccessmanager xxxxxxxx xxxxxxxx p patrol pddsitr PDDUSER repository scanner xxxxxxxx xxxxxxxx xxxxxxxx test tomcat6 u user1 Utente1 Utente2 Utente3 Utente4 Utente5 UtentePublisher	ActiveDirectorySITRS[11]	<nessun gruppo a parte Laboratorio, privilegi e risorse assegnati singolarmente, vedi Tabella 9>

[11] Gli utenti del dominio SITRS sono strutturati in Unità Organizzative (che contengono gruppi e utenti). Quelle create ad hoc sono:

- Citrix (CoreCitrix, xxxxxxxx,xxxxxxxx,xxxxxxxx,xxxxxxxx,xxxxxxxx)
- Middle (middleaccessmanager, pddsitr, PDDUSER)
- Pogest (xxxxxxxx, xxxxxxxx)

utente	dominio	gruppo/ruolo
UtenteSubscriber UtenteWfVeCo		
adminlab4 xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx	ActiveDirectorySITRS	laboratorio
xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx	ActiveDirectorySITRS	CoreCitrix
METADATI IDT CAT_READER IDT_READER SDE SDE2 RASPOI RASPOIREAD RASTURISMO SIT SIT_ADM SIT_READER CONSRAS PPR_READER METADATI_READER OSSPPR OSSPPR08	Oracle	Si usano solo ruoli di sistema.
Admin xxxxxxxx xxxxxxxx	RepositoryManager	Admin
UTENTEPUC	RepositoryManager	PUC
090003 … 107023 (377) 20090 … 20107 (6) pucga	RepositoryManager	PUCGA
Test_Com Trasm_Com Trasm_Com_2	RepositoryManager	Trasm_com
Test_Reg Trasm_Reg	RepositoryManager	Trasm_reg
user02	RepositoryManager	Tur_adm
xxxxxxxx turismo user01 user04	RepositoryManager	Tur_all
user03	RepositoryManager	Tur_cons
userpoi05 user05	RepositoryManager	Tur_void
archivio	RepositoryManager	archivio
cfva	RepositoryManager	cfva
ctr	RepositoryManager	ctr
dbtopo	RepositoryManager	dbtopo
download	RepositoryManager	download
fotocoste	RepositoryManager	fotocoste
geoweb	RepositoryManager	geoweb
metadati	RepositoryManager	metadati
poiprod poitest userpoi01 userpoi04	RepositoryManager	poi
userpoi02	RepositoryManager	poiadm
museipoi userpoi03	RepositoryManager	poiges

utente	dominio	gruppo/ruolo
ppr ppr_metadati	RepositoryManager	ppr
ppr_admin	RepositoryManager	ppr_admin
prae	RepositoryManager	prae
testPUC	RepositoryManager	testPUC
xxxxxxxx toponimi	RepositoryManager	toponimi
topoweb	RepositoryManager	topoweb
web xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx	RepositoryManager	web
webtest	RepositoryManager	webtest
manager[12]	Tomcat	manager (built-in)
Admin	ArcIMS	<ruolo unico>

Tabella 21 - Utenti attuali

* ATTENZIONE: esiste anche il dominio windows COMUNIRAS, che non è in trust con SITRs o UFFICIOPIANO, ma da cui però si può accedere anche ai server SITR.

2.7.3. Utenti futuri

Saranno definiti utenti personali (associati alle persone fisiche in relazione 1:1) e utenti applicativi, utilizzati dalle applicazioni per accedere alle risorse di cui hanno bisogno nel caso in cui non si riesca ad utilizzare quello personale dell'utente fisico che sta utilizzando l'applicazione.

Per le applicazioni three-tier, che mantengono le credenziali utente all'interno dell'application server, l'utilizzo di un utente applicativo è ritenuto sufficientemente sicuro.

Partendo dall'ipotesi di riuscire ad unificare il repository di utenti di Active Directory con quello di Oracle (in questo caso sarebbe Active Directory il repository master) sono possibili due diversi scenari:

- un solo dominio Windows
- due domini Windows trusted (come è attualmente).

Nel primo caso la convenzione per i nomi va ovviamente concordata con chi gestisce il Domain Controller di UFFICIOPIANO che è esterno al SITR.

Nel secondo caso si potrebbe utilizzare una convenzione propria, basata ad esempio sui codici fiscale:

- Utenti personali
  - UserID = CF Es. **PZZSFN64E27H199Y**
- Utenti applicativi
  - UserID = 000-APP-<codice applicazione>-000, 000-SRV-<codice servizio>-000

[12] Il nome del ruolo "manager" di Tomcat non può essere modificato. Può quindi sorgere un problema qualora si configuri la gestione dell'autenticazione di Tomcat su LDAP dove risiedono tutti i ruoli della IDT ed il nome "manager" potrebbe essere inadeguato

Es. **000-APP-0001-000**

Anche in questo ultimo caso avremmo comunque una situazione ibrida poiché utenti del dominio UFFICIOPIANO devono poter accedere alla banca dati Oracle, dove avremmo quindi utenti definiti secondo la convenzione SITR e utenti definiti secondo la convenzione del dominio UFFICIOPIANO che attualmente prevede:

- Utenti personali
  - UserID = <nome cognome> Es. **xxxxxxxx**
- Utenti applicativi
  - UserID <nessuna regola>

Si propone quindi di utilizzare in ogni caso una convenzione del tipo:

- Utenti personali
  - UserID = <nomecognome> Es. **xxxxxxxx**
- Utenti applicativi
  - UserID sitr-app-<prog> o sitr-srv-<prog>

Nella numerazione degli utenti applicativi il progressivo è quello che corrisponde al codice applicazione.

Esisteranno anche utenti Oracle non utilizzati dalle applicazioni, ma creati solo per contenere dati e altri oggetti di database. Questi utenti dovranno essere utilizzati solo nella fase di creazione degli oggetti dopodiché per la loro gestione dovranno essere utilizzati utenti personali o applicativi con i privilegi opportuni.
Questi utenti esisteranno solamente nella directory di Oracle e non in Active Directory; i loro nomi saranno liberi (lunghezza max 30ch) come ad esempio "IDT", "FC", "METADATI".

Nel caso in cui l'integrazione dei repository si effettui attraverso il protocollo Kerberos, è necessario definire in Active Directory anche utenti che rappresentano i servizi da proteggere (servizio inteso in terminologia Kerberos). In particolare va definito un utente che rappresenta il servizio Oracle. La regola per denominare tale utente sarà:

- Utenti kerberos
  - UserID = sitr-krb-<nome servizio> Es. **sitr-krb-oracle**

Il tipo di autenticazione scelta è quella "debole", basata cioè solo su user id e una password.

utente	dominio
<utente personale>	GestoreFeatureCatalogue
<utente personale>	GestoreMetadati
METADATI IDT FC SDE <utenti personali>	Oracle

sitr-app-0001 (GestoreMetadati) sitr-app-0002 (GestoreFeatureCatalogue) sitr-srv-0001 (MetadatiISO)	
<utenti personali>	ActiveDirectorySITRS
<utenti applicativi>	ActiveDirectorySITRS
<utenti personali>	RepositoryManager
<utenti personali>	Tomcat

Tabella 22 - Utenti futuri

2.7.4. Interventi

- Eliminazione di tutti gli utenti applicativi ad esclusione di
  - Dominio Oracle: quelli corrispondenti agli schemi del DB Unico.
  - Dominio Oracle: quelli corrispondenti alle applicazioni GestoreTurismo e GestorePOI (fuori dal perimetro di intervento)
  - Dominio Oracle: utente SDE (utilizzato da ArcSDE).
  - Dominio Repertorio: quelli utilizzati da GestionePUC (fuori dal perimetro di intervento)

  e loro sostituzione con utenti applicativi associati alle singole applicazioni, con nome standard e privilegi ridotti al minimo.

- Eliminazione utente SDE2

2.8. Identificazione Azioni

Le azioni sono le attività che si possono eseguire su di una risorsa, assogettabili a controllo di sicurezza e quindi intese come attività elementari, al di sotto della cui granularità non è possible andare.
Ad esempio, su di una tabella Oracle è possibile eseguire (e controllare singolarmente l'autorizzazione ad eseguire) asione di lettura record (READ), inserimento record (INSERT), cancellazione record (DELETE) e modifica record (UPDATE).

Regole di nomenclatura:

```
<NSS> ::= "act:" <TYPE> "-" <NAME>
<TYPE> ::= "app|srv|dts|dbo|dbs|fso|lyr|map|ftc|ftl|sde|dir|tml|dss"
<NAME> ::= <string>
```

Le azioni sono raggruppabili per tipo risorsa.

ResourceType	Azioni	Descr Azione
app	urn:sitr:act:app-0001-access	Accesso all'applicazione GestoreMetadati
	urn:sitr:act:app-0002-access	Accesso all'applicazione GestoreFeatureCatalogue
	urn:sitr:act:app-0004-admin	Amministratore Geoserver-1
	urn:sitr:act:app-0000-mgrtmc	Amministratore Tomcat
	urn:sitr:act:app-0009-admin	Amministratore ArcIMS
	urn:sitr:act:app-0000-mgralb	Manager Apache LB
	urn:sitr:act:app-0013-dba	Amministratore Oracle
	urn:sitr:act:app-0015-admin	Amministratore Active Directory

ResourceType	Azioni	Descr Azione
	urn:sitr:act:app-0019-main	Accesso a Sardegna2D
	urn:sitr:act:app-0021-admsrv	Gestione servizi WMS ArcIMS
	urn:sitr:act:app-0022-admsrv	Gestione servizi WMS ArcIMS
	urn:sitr:act:app-0023-read	Repertorio: lettura
	urn:sitr:act:app-0023-readmap	Repertorio: lettura mappe
	urn:sitr:act:app-0023-readrel	Repertorio: lettura relazioni
	urn:sitr:act:app-0023-readtab	Repertorio: lettura tabelle alfa
	urn:sitr:act:app-0023-write	Repertorio: scrittura
	urn:sitr:act:app-0023-writent	Repertorio: scrittura entità grafiche
	urn:sitr:act:app-0023-writemap	Repertorio: scrittura mappe
	urn:sitr:act:app-0023-writemd	Repertorio: scrittura metadati
	urn:sitr:act:app-0023-writepar	Repertorio: scrittura parametri
	urn:sitr:act:app-0023-writerel	Repertorio: scrittura relazioni
	urn:sitr:act:app-0023-print	Repertorio: stampa
	urn:sitr:act:app-0023-pub	Repertorio: pubblicazioni
	urn:sitr:act:app-0023-security	Repertorio: sicurezza
	urn:sitr:act:app-0025-access	
	urn:sitr:act:app-0029-admin	Amministrazione mySQL
	urn:sitr:act:app-0034-access	
	urn:sitr:act:app-0035-access	
	urn:sitr:act:app-0036-read	
	urn:sitr:act:app-0036-write	
	urn:sitr:act:app-0037-access	
	urn:sitr:act:app-0037-admin	
	urn:sitr:act:app-0101-accetl1	Attivazione ETL 1
	...	…
	urn:sitr:act:app-0229-accetl229	Attivazione ETL 119
aps	urn:sitr:act:aps-access-1	Attivazione ETL del gruppo 1
	...	…
	urn:sitr:act:aps-access-15	Attivazione ETL del gruppo 15
	urn:sitr:act:aps-admin-101	Amministrazione Tomcat
	urn:sitr:act:aps-admin-102	Amministrazione JBOSS
	urn:sitr:act:aps-admin-103	Amministrazione Apache LB
	urn:sitr:act:aps-admin-104	Amminsitrazione WMS Connector
	urn:sitr:act:aps-admin-105	Amministrazione Geoserver
srv	urn:sitr:act:srv-0001-access	WMS Geoserver
	urn:sitr:act:srv-0002-access	WMS ArcIMS (pubblico)
	urn:sitr:act:srv-0003-access	WMS ArcIMS (private)
	urn:sitr:act:srv-0004-access	WFS Geoserver
dbo	urn:sitr:act:dbo-select	Lettura record tabella o vista Oracle
	urn:sitr:act:dbo-insert	Inserimento record tabella o vista Oracle
	urn:sitr:act:dbo-update	Aggiornamento record tabella o vista Oracle
	urn:sitr:act:dbo-delete	Eliminazione record tabella o vista Oracle
fso	urn:sitr:act:fso-read	Lettura file
	urn:sitr:act:fso-write	Scrittura file
	urn:sitr:act:fso-full	FullControl
	urn:sitr:act:fso-change	Modifica
	urn:sitr:act:fso-reade_ex	Lettura ed esecuzione
	urn:sitr:act:fso-list_folder	Contenuto cartelle
dir	urn:sitr:act:dir-full	FullControl
	urn:sitr:act:dir-modi	Modify
	urn:sitr:act:dir-rexe	Read/Execute
	urn:sitr:act:dir-list	ListFolderContent
	urn:sitr:act:dir-read	Read
	urn:sitr:act:dir-write	Write

ResourceType	Azioni	Descr Azione
dts	urn:sitr:act:dts-select	Lettura record tabella o vista Oracle/Lettura file
	urn:sitr:act:dts-insert	Inserimento record tabella o vista Oracle/Scrittura file
	urn:sitr:act:dts-update	Eliminazione record tabella o vista Oracle/Scrittura file
	urn:sitr:act:dts-delete	Eliminazione record tabella o vista Oracle/Scrittura file
dbs	urn:sitr:act:dbs-select	Lettura record tabella o vista Oracle contenuta nello schema
	urn:sitr:act:dbs-insert	Inserimento record tabella o vista Oracle contenuta nello schema
	urn:sitr:act:dbs-update	Eliminazione record tabella o vista Oracle contenuta nello schema
	urn:sitr:act:dbs-delete	Eliminazione record tabella o vista Oracle contenuta nello schema
	urn:sitr:act:dbs-resource	Creazione oggetti nello schema
lyr	urn:sitr:act:lyr-cap	Layer presente nella GetCapabilities
	urn:sitr:act:lyr-map	GetMap
	urn:sitr:act:lyr-inf	GetFeatureInfo
map	urn:sitr:act:map-cap	Layer presente nella GetCapabilities
	urn:sitr:act:map-map	GetMap
	urn:sitr:act:map-inf	GetFeatureInfo
	urn:sitr:act:map-s2d-main[13]	Visualizzazione su S2D
	urn:sitr:act:map-s2d-delfil	Visualizzazione su S2D: disattivazione filtro
	urn:sitr:act:map-s2d-info	Visualizzazione su S2D: info feature
	urn:sitr:act:map-s2d-misarea	Visualizzazione su S2D: misurazione area
	urn:sitr:act:map-s2d-mislung	Visualizzazione su S2D: misurazione lunghezza
	urn:sitr:act:map-s2d-md	Visualizzazione su S2D: collegamento a metadati
	urn:sitr:act:map-s2d-pdf	Visualizzazione su S2D: stampa pdf
	urn:sitr:act:map-s2d-fullscr	Visualizzazione su S2D: full screen
	urn:sitr:act:map-s2d-selcir	Visualizzazione su S2D: selezione circolare
	urn:sitr:act:map-s2d-selret	Visualizzazione su S2D: selezione rettangolare
	urn:sitr:act:map-s2d-selpol	Visualizzazione su S2D: selezione poligonale
	urn:sitr:act:map-s2d-delsel	Visualizzazione su S2D: disattivazione selezione
	urn:sitr:act:map-sm-main	Visualizzazione su SardegnaMappe.
ftc	urn:sitr:act:ftc-cap	Feature Type presente nella GetCapabilities
	urn:sitr:act:ftc-des	DescribeFeatureType
	urn:sitr:act:ftc-get	GetFeature
ftl	urn:sitr:act:ftl-cap	Feature Type presente nella GetCapabilities
	urn:sitr:act:ftl-des	DescribeFeatureType
	urn:sitr:act:ftl-get	GetFeature
sde	urn:sitr:act:sde-select	Lettura record tabella o vista SDE
	urn:sitr:act:sde-update	Update record tabella o vista SDE
	urn:sitr:act:sde-insert	Inserimento record tabella o vista SDE
	urn:sitr:act:sde-delete	Cancellazione record tabella o vista SDE
dss	urn:sitr:act:dss-select	Lettura record tabella o vista SDE
	urn:sitr:act:dss-update	Update record tabella o vista SDE
	urn:sitr:act:dss-insert	Inserimento record tabella o vista SDE
	urn:sitr:act:dss-delete	Cancellazione record tabella o vista SDE

[13] Le azioni relative alla visualizzazione e altre funzionalità di Sardegna2D si applicano a mappe implementate come map service ArcIMS, così come le azioni di visualizzazione attraverso SardegnaMappe si applicano solamente a quelle configurate in SaredegnaMappe. Tali azioni sono state attribuite alle mappe piuttosto che all'applicazione Sardegna2D perché sono inevitabilmente collegate ai dati visualizzati attraverso il meccanismo di gestione delle autorizzazioni del Repertorio.

ResourceType	Azioni	Descr Azione
tml	urn:sitr:act:tml-map	Visualizzazione tasselli TMS

Tabella 23 - Elenco azioni

2.9. Identificazione profili

In questo capitolo elencheremo gli attuali profili o ruoli di autorizzazione presenti, laddove identificabili come tali nel contesto di un dominio di autenticazione/autorizzazione e quelli impliciti, dove invece non viene gestito il concetto di ruolo (ad esempio, nel GestoreFeatureCatalogue sono gestiti solamente gli utenti).
Definiremo poi una proposta di profili a cui tendere, in un contesto ideale di un unico dominio di A/A. Tali profili saranno inoltre descritti attraverso il set di Policy ad essi assegnati ed infine tali policy saranno mappate sui meccanismi attuali di sicurezza, per consentirne una implementazione immediata, senza ancora raggiungere l'unicità del dominio.
Successivamente i termini ruolo o profilo saranno utilizzati in maniera interscambiabile, intendendo sempre per ruolo il "ruolo funzionale" e non quello organizzativo.

2.9.1. Profili attuali

Laddove esiste un concetto assimilabile al profilo/ruolo (vedi ad esempio il concetto di "profilo" del Repertorio Metadati Applicativi) verrà indicato il nome di questo concetto. Negli altri casi verrà indicato un nome tra parentesi acute <nome_profilo> con il significato di ruolo virtuale.

Nome profilo	Cosa può fare	Dominio
metadati	Editare metadati	GestoreMetadati
web[14]	Consultazione mappa generica su Sardegna2D	Repertorio
scarico[15]		Repertorio
puc[16]	Consultazione mappa PUC su Sardegna2D	Repertorio
dbtopo[17]	Consultazione mappa DB topografico su Sardegna2D	Repertorio
<editor_fc>	Editare feature catalogue	FeatureCatalogue
<tutti>	Consultare feature catalogue Consultare metadati Consultare servizi OWS Consultare servizi TMS Consultare Sardegna2D (vedi profili web, puc, dbtopo)	-
ROLE_CATASTO	Consultare WMS/WFS dati catastali.	Geoserver
ROLE_ADMINISTRATOR	Catalogare nuove Feature Type, stili, datastore …	Geoserver

[14] Questo profilo esiste nel Repertorio, ma l'utente ad esso collegato è utilizzato in maniera trasparente da tutti gli utenti che accedono all'applicazione senza identificarsi. Serve a identificare i layer e le funzionalità disponibili all'intetrno di Sardegna2D
[15] Questo profilo esiste nel Repertorio, ma l'utente ad esso collegato è utilizzato in maniera trasparente da tutti gli utenti che accedono all'applicazione senza identificarsi. Serve a identificare i dati disponibili per l'estrazione on-line dei dati vettoriali della IDT attraverso l'applicazione ScaricoCartografia.
[16] Idem come nota 14.
[17] Idem come nota 14.

	Profilo built-in di Geoserver. Stop, avvio, refresh servizi OWS.	
<*manager*>	Stop, avvio, refresh, deploy, undeploy di applicazioni web	Tomcat
<*administrator*>	Stop, avvio, refresh, creazione, cancellazione servizi di mappa ArcIMS	ArcIMS
<*administrator*>	Avvio, Stop interfaccia WMS su servizi di mappa ArcIMS esistenti.	WMSConnector
<*manager*>[18]	Modifica opzioni di bilanciamento delle richieste verso gli application server.	ApacheLoadBalancer
Administrators	Gestione utenti. Gestione autorizzazioni.	ActiveDirectory

Tabella 24 - Profili attuali

2.9.2. Profili futuri

In questo paragrafo viene indicata una proposta di profili futuri, specificando se tale profilo è per utenti umani o applicativi. La descrizione delle autorizzazioni associate a ciascun profilo è fatta in linguaggio naturale.

Nome profilo	Tipo	Codice	Cosa deve fare
role_idt_anonymous	U/A	urn:sitr:pro:0001-anonymous	Accede ai dati DB Unico liberi tramite applicazioni e servizi in sola lettura esposti sulla rete pubblica.
role_idt_free_direct_read	U/A	urn:sitr:pro:0002-free-direct-read	Accede ai dati liberi del DB Unico in modalità diretta in sola lettura
role_idt_ catasto_direct_read	U/A	urn:sitr:pro:0003-catasto-direct-read	Accede ai dati del catasto del DB Unico in modalità diretta in sola lettura
role_idt_catasto_ows_read	U/A	urn:sitr:pro:0004-idt-role-catasto-ows-read	Accede ai dati del catasto del DB Unico in modalità ows in sola lettura
role_idt_md_manage	U	urn:sitr:pro:0005-md-manage	Gestore dei metadati
role_idt_fc_manage	U	urn:sitr:pro:0006-fc-manage	Gestore del Feature Catalogue
role_idt_security_admin	U	urn:sitr:pro:0007-security-admin	Amministratore sicurezza IDT (Active Directory)
role_idt_sys_admin	U	urn:sitr:pro:0008-sys-admin	Amministratore sistemi della IDT (tomcat, apache, oracle)
role_idt_geo_admin	U	urn:sitr:pro:0009-geo-admin	Amministratore sw di base della IDT (Geoserver, ArcIMS)
role_idt_app_md_read	A	urn:sitr:pro:0010-app-md-read	Lettura dello schema metadati
role_idt_app_md_write	A	urn:sitr:pro:0011-app-md-write	Scrittura dello schema metadati
role_idt_app_fc_read	A	urn:sitr:pro:0012-app-fc-read	Lettura dello schema feature catalogue
role_idt_app_fc_write	A	urn:sitr:pro:0013-app-fc-write	Scrittura dello schema feature catalogue

[18] Attualmente l'accesso a tale funzionalità non viene controllata con l'identificazione di un utente, ma attraverso un filtro sugli IP.

Nome profilo	Tipo	Codice	Cosa deve fare
role_idt_free_sde_read	U/A	urn:sitr:pro:0014-free-sde-read	Accede ai dati liberi del DB Unico in modalità sde in sola lettura
role_idt_catasto_sde_read	U/A	urn:sitr:pro:0015-catasto-sde-read	Accede ai dati del catasto del DB Unico in modalità sde in sola lettura
role_idt_mdw_exec	A	urn:sitr:pro:0051-app-service-exec	Esecuzione processi Middleware
role_idt_etl_exec	U/A	urn:sitr:pro:0052-app-etl-exec	Esecuzione processi di ETL
role_idt_app_etl_01_writer	A	urn:sitr:pro:0101-app-etl-01-writer	Scrittura delle FT del dataset "01"
…	A	…	…
role_idt_app_etl_15_writer	A	urn:sitr:pro:0115-app-etl-15-writer	Scrittura delle FT del dataset "15"
role_idt_fs_01_reader	A/U	urn:sitr:pro:0201-fs-01-reader	Lettura dati su file system, cartella "01"
…	…	…	…
role_idt_fs_19_reader	A/U	urn:sitr:pro:0219-fs-01-reader	Lettura dati su file system, cartella "19"
role_idt_fs_01_writer	A/U	urn:sitr:pro:0301-fs-01-writer	Scrittura dati su file system, cartella "01"
…	…	…	…
role_idt_fs_19_writer	A/U	urn:sitr:pro:0319-fs-01-writer	Scrittura dati su file system, cartella "19"

Tabella 25 - Profili futuri

ATTENZIONE: ci possono essere problemi nel momento in cui un amministratore di sw di base può anche interagire con il sistema locale di sicurezza nel caso in cui non si possano disabilitare queste funzioni. Per fare un esempio: un amministratore di Geoserver potrebbe dare o togliere privilegi incoerentemente con quanto deciso dall'amministratore della sicurezza poiché un amministratore di Geoserver ha sempre a disposizione le funzionalità di gestione della sicurezza locale.

Le policy che definiscono i profili suddetti sono elencate nella seguente **Tabella 26**

Profilo	azione	risorsa
urn:sitr:pro:0001-anonymous Accede ai dati DB Unico liberi tramite applicazioni e servizi in sola lettura esposti sulla rete pubblica.		
Accede al WMS di Geoserver	urn:sitr:act:srv-0001-access[19]	urn:sitr:res:srv-0001-WMS-1
Accede al WMS di ArcIMS (pubblico)	urn:sitr:act:srv-0002-access	urn:sitr:res:srv-0002-WMS-1
Accede al WFS di Geoserver	urn:sitr:act:srv-0004-access	urn:sitr:res:srv-0004-WFS-1
Esegue la GetCapabilities WMS su tutti I layer della mappa "dbu"	urn:sitr:act:map-cap	urn:sitr:res:map-0002-dbu
Esegue la GetMap WMS su tutti I layer della mappa	urn:sitr:act:map-map	urn:sitr:res:map-0002-dbu

[19] L'attuale implementazione del controllo degli accessi di Geoserver non consente in realtà di gestire contemporaneamente policy sui servizi e sui layer/feature type erogati dai servizi stessi.

Profilo	azione	risorsa
"dbu"		
Esegue la GetFeatureInfo su tutti I layer della mappa "dbu"	urn:sitr:act:map-inf	urn:sitr:res:map-0002-dbu
Esegue la GetCapabilities WMS su tutti I layer della mappa "ortofoto"	urn:sitr:act:map-cap	urn:sitr:res:map-0003-ortofoto
Esegue la GetMap WMS su tutti I layer della mappa "ortofoto"	urn:sitr:act:map-map	urn:sitr:res:map-0003-ortofoto
Esegue la GetFeatureInfo su tutti I layer della mappa "ortofoto"	urn:sitr:act:map-inf	urn:sitr:res:map-0003-ortofoto
Esegue la GetCapabilities WFS su tutte le FT della FeatureList "dbu"	urn:sitr:act:ftc-cap	urn:sitr:res:ftl-0002-dbu
Esegue la DescribeFeature WFS su tutte le FT della FeatureList "dbu"	urn:sitr:act:ftc-des	urn:sitr:res:ftl-0002-dbu
Esegue la GetFeatures WFS su tutte le FT della FeatureList "dbu"	urn:sitr:act:ftc-get	urn:sitr:res:ftl-0002-dbu
Esegue l'accesso all'applicazione CatalogoDati	*<nessuna azione disponibile>*	urn:sitr:res:app-0003-CatalogoDati
Esegue l'accesso in all'applicazione FeatureCatalogue	*<nessuna azione disponibile>*	urn:sitr:res:app-0012-FeatureCatalogue
Sardegna2D: accesso all'applicazione	urn:sitr:act:app-0019-main	urn:sitr:res:app-0019-Sardegna2D
Visualizzazione cartografia di base su Sardegna2D	urn:sitr:act:map-s2d-main	urn:sitr:res:map-0026-aims1
Visualizzazione DBTOPO su Sardegna2D	urn:sitr:act:map-s2d-main	urn:sitr:res:map-0028-aims3
Visualizzazione PPR su Sardegna2D	urn:sitr:act:map-s2d-main	urn:sitr:res:map-0029-aims4
Visualizzazione stradario su SardegnaMappe	urn:sitr:act:map-sm-main	urn:sitr:res:map-0005-tms2
Visualizzazione stradario trasparente su SardegnaMappe	urn:sitr:act:map-sm-main	urn:sitr:res:map-0006-tms3
Visualizzazione ortofoto 2006 su SardegnaMappe	urn:sitr:act:map-sm-main	urn:sitr:res:map-0004-tms1
urn:sitr:pro:0002-free-direct-read		
	urn:sitr:act:dts-select	urn:sitr:res:dts-0002-DB10K
	urn:sitr:act:dts-select	urn:sitr:res:dts-0003-CartaGeologica
	urn:sitr:act:dts-select	urn:sitr:res:dts-0004-POI
	urn:sitr:act:dts-select	urn:sitr:res:dts-0005-EnteForeste
	urn:sitr:act:dts-select	urn:sitr:res:dts-0006-QuadriUnione
	urn:sitr:act:dts-select	urn:sitr:res:dts-0007-AcquePubbliche
	urn:sitr:act:dts-select	urn:sitr:res:dts-0008-PPR
	urn:sitr:act:dts-select	urn:sitr:res:dts-0009-FasceRispetto

Profilo	azione	risorsa
	urn:sitr:act:dts-select	urn:sitr:res:dts-0010-UsoSuolo
	urn:sitr:act:dts-select	urn:sitr:res:dts-0011-AmbitiAmministrativi
	urn:sitr:act:dts-select	urn:sitr:res:dts-0012-CFVA
	urn:sitr:act:dts-select	urn:sitr:res:dts-0013-ProtezioneCivile
	urn:sitr:act:dts-select	urn:sitr:res:dts-0014-LavoriPubblici
	urn:sitr:act:dts-select	urn:sitr:res:dts-0015-FotoAeree
	urn:sitr:act:dss-select	urn:sitr:res:dss-0002-DB10K
	urn:sitr:act:dss-select	urn:sitr:res:dss-0003-CartaGeologica
	urn:sitr:act:dss-select	urn:sitr:res:dss-0004-POI
	urn:sitr:act:dss-select	urn:sitr:res:dss-0005-EnteForeste
	urn:sitr:act:dss-select	urn:sitr:res:dss-0006-QuadriUnione
	urn:sitr:act:dss-select	urn:sitr:res:dss-0007-AcquePubbliche
	urn:sitr:act:dss-select	urn:sitr:res:dss-0008-PPR
	urn:sitr:act:dss-select	urn:sitr:res:dss-0009-FasceRispetto
	urn:sitr:act:dss-select	urn:sitr:res:dss-0010-UsoSuolo
	urn:sitr:act:dss-select	urn:sitr:res:dss-0011-AmbitiAmministrativi
	urn:sitr:act:dss-select	urn:sitr:res:dss-0012-CFVA
	urn:sitr:act:dss-select	urn:sitr:res:dss-0013-ProtezioneCivile
	urn:sitr:act:dss-select	urn:sitr:res:dss-0014-LavoriPubblici
urn:sitr:pro:0003-catasto-direct-read	urn:sitr:act:dts-select	urn:sitr:res:dts-0001-Catasto
	urn:sitr:act:dss-select	urn:sitr:res:dss-0001-Catasto
urn:sitr:pro:0004-idt-role-catasto-ows-read	urn:sitr:act:srv-0001-access	urn:sitr:res:srv-0001-WMS-1
	urn:sitr:act:srv-0004-access	urn:sitr:res:srv-0004-WFS-1
	urn:sitr:act:map-cap	urn:sitr:res:map-0001-cat
	urn:sitr:act:map-map	urn:sitr:res:map-0001-cat
	urn:sitr:act:map-inf	urn:sitr:res:map-0001-cat
	urn:sitr:act:ftc-cap	urn:sitr:res:ftl-0001-cat
	urn:sitr:act:ftc-des	urn:sitr:res:ftl-0001-cat
	urn:sitr:act:ftc-get	urn:sitr:res:ftl-0001-cat
urn:sitr:pro:0005-md-manage[20]	urn:sitr:act:app-0001-access	urn:sitr:res:app-0001-GestoreMetadati
	urn:sitr:act:dbs-select	urn:sitr:res:dbs:0002-md
	urn:sitr:act:dbs-insert	urn:sitr:res:dbs:0002-md

[20] Si ipotizza che l'utente dell'applicazione GestoreMetadati sia lo stesso utente utilizzato per stabilire la connessione al DB; sono necessarie quindi le policy relative alle tabelle dello schema.

Profilo	azione	risorsa
	urn:sitr:act:dbs-update	urn:sitr:res:dbs:0002-md
	urn:sitr:act:dbs-delete	urn:sitr:res:dbs:0002-md
urn:sitr:pro:0006-fc-manage[21]	urn:sitr:act:app-0002-access	urn:sitr:res:app-0002-GestoreFeatureCatalogue
urn:sitr:pro:0007-security-admin	urn:sitr:act:app-0015-admin	urn:sitr:res:app-0015-ActiveDirectory
	urn:sitr:act:app-0013-dba	urn:sitr:res:app-0015-Oracle
	urn:sitr:act:app-0023-security	urn:sitr:res:app-0023-RepositoryManager
urn:sitr:pro:0008-sys-admin	urn:sitr:act:aps-admin-103	urn:sitr:res:aps-0103-MW-Apache
	urn:sitr:act:aps-admin-101	urn:sitr:res:aps-0101-MW-Tomcat
	urn:sitr:act:app-0029-admin	urn:sitr:res:app-0029-MySQLAdmin
urn:sitr:pro:0009-geo-admin	urn:sitr:act:aps-admin-105	urn:sitr:res:aps-0105-Geoserver
	urn:sitr:act:aps-admin-104	urn:sitr:res:aps-0105-WMSConnector
	urn:sitr:act:app-0009-admin	urn:sitr:res:app-0009-ArcIMSAdmin
	urn:sitr:act:app-0023-read	urn:sitr:res:app-0023-RepositoryManager
	urn:sitr:act:app-0023-readmap	urn:sitr:res:app-0023-RepositoryManager
	urn:sitr:act:app-0023-readrel	urn:sitr:res:app-0023-RepositoryManager
	urn:sitr:act:app-0023-readtab	urn:sitr:res:app-0023-RepositoryManager
	urn:sitr:act:app-0023-write	urn:sitr:res:app-0023-RepositoryManager
	urn:sitr:act:app-0023-writent	urn:sitr:res:app-0023-RepositoryManager
	urn:sitr:act:app-0023-writemap	urn:sitr:res:app-0023-RepositoryManager
	urn:sitr:act:app-0023-writemd	urn:sitr:res:app-0023-RepositoryManager
	urn:sitr:act:app-0023-writepar	urn:sitr:res:app-0023-RepositoryManager
	urn:sitr:act:app-0023-writerel	urn:sitr:res:app-0023-RepositoryManager
	urn:sitr:act:app-0023-print	urn:sitr:res:app-0023-RepositoryManager
	urn:sitr:act:app-0023-pub	urn:sitr:res:app-0023-RepositoryManager
urn:sitr:pro:0010-app-md-read	urn:sitr:act:dbs-select	urn:sitr:res:dbs:0002-md
urn:sitr:pro:0011-app-md-write	urn:sitr:act:dbs-select	urn:sitr:res:dbs:0002-md
	urn:sitr:act:dbs-insert	urn:sitr:res:dbs:0002-md
	urn:sitr:act:dbs-update	urn:sitr:res:dbs:0002-md

[21] La tecnologia server dell'applicazione fa sì che l'utente usato per accedere all'applicazione non sia lo stesso utilizzato dall'applicazione per stabilire la connessione al DB. Non è necessario quindi aggiungere policy relative allo schema dati dell'applicazione.

Profilo	azione	risorsa
	urn:sitr:act:dbs-delete	urn:sitr:res:dbs:0002-md
urn:sitr:pro:0012-app-fc-read	urn:sitr:act:dbs-select	urn:sitr:res:dbs:0005-fc
urn:sitr:pro:0013-app-fc-write	urn:sitr:act:dbs-insert	urn:sitr:res:dbs:0005-fc
	urn:sitr:act:dbs-update	urn:sitr:res:dbs:0005-fc
	urn:sitr:act:dbs-delete	urn:sitr:res:dbs:0005-fc
	urn:sitr:act:dbs-select	urn:sitr:res:dbs:0005-fc
urn:sitr:pro:0014-free-sde-read	urn:sitr:act:dss-select	urn:sitr:res:dss-0002-DB10K
	urn:sitr:act:dss-select	urn:sitr:res:dss-0003-CartaGeologica
	urn:sitr:act:dss-select	urn:sitr:res:dss-0004-POI
	urn:sitr:act:dss-select	urn:sitr:res:dss-0005-EnteForeste
	urn:sitr:act:dss-select	urn:sitr:res:dss-0006-QuadriUnione
	urn:sitr:act:dss-select	urn:sitr:res:dss-0007-AcquePubbliche
	urn:sitr:act:dss-select	urn:sitr:res:dss-0008-PPR
	urn:sitr:act:dss-select	urn:sitr:res:dss-0009-FasceRispetto
	urn:sitr:act:dss-select	urn:sitr:res:dss-0010-UsoSuolo
	urn:sitr:act:dss-select	urn:sitr:res:dss-0011-AmbitiAmministrativi
	urn:sitr:act:dss-select	urn:sitr:res:dss-0012-CFVA
	urn:sitr:act:dss-select	urn:sitr:res:dss-0013-ProtezioneCivile
	urn:sitr:act:dss-select	urn:sitr:res:dss-0014-LavoriPubblici
urn:sitr:pro:0015-catasto-sde-read	urn:sitr:act:dss-select	urn:sitr:res:dss-0001-Catasto
urn:sitr:pro:0051-app-service-exec	urn:sitr:act:dir-full	urn:sitr:res:dir:0010-dati
	urn:sitr:act:dir-full	urn:sitr:res:dir:0012-geoblog
	urn:sitr:act:dir-full	urn:sitr:res:dir:0013-geoscat
	urn:sitr:act:dir-full	urn:sitr:res:dir:0014-gwc
	urn:sitr:act:dir-full	urn:sitr:res:dir:0016-scarico
	urn:sitr:act:dir-full	urn:sitr:res:dir:0017-scartmp
urn:sitr:pro:0101-app-etl-01-writer	urn:sitr:act:dss-select	urn:sitr:res:dss-0001-Catasto
	urn:sitr:act:dss-insert	urn:sitr:res:dss-0001-Catasto
	urn:sitr:act:dss-delete	urn:sitr:res:dss-0001-Catasto
	urn:sitr:act:dss-update	urn:sitr:res:dss-0001-Catasto
…	urn:sitr:act:dbs-resource	urn:sitr:res:dbs:0001-idt
urn:sitr:pro:0115-app-etl-15-writer	urn:sitr:act:fso-full	urn:sitr:res:dir:0010-dati

Profilo	azione	risorsa
urn:sitr:pro:0201-fs-01-reader	urn:sitr:act:dir-read	urn:sitr:res:dir:0001-arcims
…		
urn:sitr:pro:0219-fs-01-reader	urn:sitr:act:dir-read	urn:sitr:res:dir:0019-dboper
urn:sitr:pro:0301-fs-01-writer	urn:sitr:act:dir-full	urn:sitr:res:dir:0001-arcims
…		
urn:sitr:pro:0319-fs-01-writer	urn:sitr:act:dir-full	urn:sitr:res:dir:0019-dboper

Tabella 26 - Relazione profilo-azione-risorsa (policy)

2.9.3. Implementazione delle Policy

Per avere una modalità inequivocabile con cui descrivere gli interventi da effettuare sui sistemi esistenti per ottenere le autorizzazioni necessarie, si è cercato di usare il più possibile linguaggi codificati come SQL o script e non istruzioni discorsive o GUI di amministrazione. Nel caso particolare delle autorizzazioni per Active Directory si è scelto di fare riferimento ad una libreria di routine SetACL (http://setacl.sourceforge.net/) vista la lacuna nei comandi Windows di shell.

Per comodità, riportiamo qui di seguito il significato dei principali parametri usati dal comando SetACL:

-**ot** = tipo di risorsa (object type): file, network share …
-**on** = nome della risorsa (object name)
-**ace** = access control entry: contiene le informazioni su destinatario dell'autorizzazione, il permesso da autorizzare e altre opzioni secondarie (come la propagazione ereditaria ecc.). La sintassi per esprimere il contenuto di una ace è la seguente:

n:<trustee>**;p:**<permission>

dove

trustee = beneficiario (utente, gruppo)
permission = azioni autorizzate(dipendenti dal tipo di risorsa).

-**actn** = azione da eseguire con il comando (action); può valere:
ace = esegue quanto specificato nel parametro -ace
… = altri parametri non essenziali in questo contesto

I permessi di base per un oggetto di tipo file o cartella sono i seguenti:
- read: lettura
- write: scrittura
- list_folder: lista del contenuto della cartella
- read_ex: lettura, esecuzione
- change: modifica

- full: accesso completo

il significato di tali permessi è riassunto nella **Tabella 27**

AUTORIZZAZIONE	cartella	file
read (lettura)	Permette la visualizzazione e l'elencazione di file e sottocartelle	Permette la visualizzazione e l'accesso al contenuto del file
write (scrittura)	Permette l'aggiunta di file e sottocartelle	Permette la scrittura in un file
read_ex (lettura & esecuzione)	Permette la visualizzazione e l'elencazione di file e sottocartelle; inoltre consente l'esecuzione di file ivi contenuti.	Permette la visualizzazione, l'accesso al contenuto e l'esecuzione del file.
list_folder (visualizzazione contenuto cartelle)	Permette la visualizzazione e l'elencazione di file e sottocartelle; inoltre consente l'esecuzione di file ivi contenuti.	N/D
change (modifica)	Permette la lettura e scrittura per file e sottocartelle e consente l'eliminazione della cartella.	Permette la lettura e scrittura per il file ed anche la sua eliminazione.
full (controllo completo)	Permette la lettura e scrittura per file e sottocartelle e consente l'eliminazione di file e sottocartelle.	Permette la lettura e scrittura per il file ed anche la sua eliminazione.

Tabella 27- Autorizzazioni di base su file e cartelle

Per la creazione di utenti o gruppi si sono utilizzati i comandi di sistema NET:

NET USER …= gestione utenti
NET GROUP…= gestione gruppi

Per la gestione di utenti e ruoli e l'attribuzione di permessi di sistema e di oggetto in Oracle si utilizzano i seguenti comandi SQL:

-- Creazione di un utente
create user <user_name> identified by <password>;

-- Creazione di un ruolo
create role <role_name>;

-- assegnazione di un privilegio a un utente o a un ruolo
grant <role_name> to <user_name/role_name>;

--assegnazione di un privilegio di oggetto ad un ruolo
grant select/insert/update/delete on <object_name> to <role_name>;

--assegnazione di un insieme di privilegi ad un ruolo o ad un utente
grant <role_name> to <role_name/user_name>;

	implementazione	
Profilo	**Dominio**	**Policy**
urn:sitr:pro:0001-anonymous[22]	tutti	nessuna
urn:sitr:pro:0002-free-direct-read	Oracle	Creazione dei ruoli per ciascuno dei 14 dataset vettoriali di dati liberi: **create role ROLE_IDT_DTS02_READER;** **create role ROLE_IDT_DTS03_READER;** **…** **create role ROLE_IDT_DTS15_READER;** Creazione di un unico ruolo che racchiuda tutti i ruoli precedenti (per semplificare la gestione): **create role ROLE_IDT_DTS_FREE_READER;** **grant** **ROLE_IDT_DTS02_READER,** **ROLE_IDT_DTS03_READER,** **…** **ROLE_IDT_DTS14_READER** **to** **ROLE_IDT_DTS_FREE_READER;** Attribuzione dei privilegi di lettura ai ruoli per ciascuno degli oggetti del dataset: **grant select on** **DBTSEDETRASPORTOFERRO,** **DBTACQUEDOTTO,** **…,** **DBTVIABILITAMISTASECONDARCHI** **to** **ROLE_IDT_DTS02_READER;** … **grant select on** **PICCOLIINVASI** **to** **ROLE_IDT_DTS14_READER;** Attribuzione degli utenti al ruolo: grant ROLE_IDT_DTSFREE_READER to <user1>; grant ROLE_IDT_DTSFREE_READER to <user2>;

[22] Il ruolo anonimo è realizzato attraverso l'utilizzo di nessun account; non si effettua cioè l'autenticazione. In questo modo tutte le risorse accessibili attraverso la LAN o Oracle o SDE non sono assolutamente accessibili, mentre possono essere accedute senza identificazione alcuni servizi OWS e alcune applicazioni web.

	implementazione	
Profilo	**Dominio**	**Policy**
		…
	ActiveDirectory	Creare un utente user1 **NET USER <user1> <psswd> /ADD /DOMAIN** Creare il gruppo di utenti **NET GROUP role_idt_dts15_reader /ADD /DOMAIN** Aggiungere l'utente user1 al gruppo: **NET GROUP <user1> role_idt_dts15_reader /ADD /DOMAIN** Attribuire il privilegio di lettura sui file corrispondenti ai dati raster **SetACL.exe -on "ortofoto_it_2000.ecw" -ot file -actn ace -ace "n:SITRS\role_idt_dts15_reader;p:read"** **SetACL.exe -on "ortofoto_it_2006.ecw" -ot file -actn ace -ace "n:SITRS\role_idt_dts15_reader;p:read"** …
urn:sitr:pro:0003-catasto-direct-read	Oracle	Creazione del ruoli per il dataset vettoriale del catasto: **create role ROLE_IDT_DTS01_READER;** Attribuzione dei privilegi di lettura al ruolo per ciascuno degli oggetti del dataset: **grant select on** **ACQUECATASTO,** **CAMPITURECATASTO,** **…,** **TESTIPARTICELLECATASTO** **to** **ROLE_IDT_DTS01_READER;** Attribuzione degli utenti al ruolo: **grant** **ROLE_IDT_DTS01_READER** **to** **<user1>;** **grant** **ROLE_IDT_DTS01_READER** **to** **<user2>;** …
urn:sitr:pro:0004-idt-role-catasto-ows-read	Geoserver (HTTPS)	definire gli utenti e i ruoli: nel file GEOSERVER_DATA_DIR/security/user.properties inserire le righe admin=geoserver,ROLE_ADMINISTRATOR <user1>=<passwd>,ROLE_IDT_MAP01_READER <user2>=<passwd>,ROLE_IDT_MAP01_READER

	implementazione	
Profilo	**Dominio**	**Policy**
		definire i privilegi del ruolo, nel file: GEOSERVER_DATA_DIR/security/layers.properties mode=CHALLENGE inserire la riga cas.*.r=ROLE_IDT_MAP01_READER[23]
urn:sitr:pro:0005-md-manage	GestoreMetadati	Si tratta di inserire un record nella tabella utilizzata dall'applicazione per la gestione della sicurezza. insert into RX_UTENTE (BLOCCATO, DA_LDAP, DATA_SCAD_PWD, DATA_ULT_UTIL, ID_ENTE, LOGIN_AUTO, MODIFICA_PWD, NOME, ORG, PASSWORD, PASSWORD_CRYPT, PROFILO, RIFERIMENTO, SCAD_ULT_UTIL, VALIDITA_PWD) values (0, 0, null, to_date('16-APR-10','DD-MON-RR'), 1, 0, 0, <user1>, '01', <psswd>, <psswd_cry>, 'metadati', null, 1, 0); Volendo è possibile modificare il nome del profilo 'metadati' contenuto nella tabella RX_PROFILO in ROLE_IDT_MD_MNGR
urn:sitr:pro:0006-fc-manage	FeatureCatalogue	Come indicato nel documento SITR-DB-037(A) nel file session.properties settare Authenticator.password.<user1>=<passwd> Authenticator.password.<user2>=<passwd> Non è implementato il concetto di ruolo.

[23] Il gruppo di layer catasto è individuato in Geoserver dal namespace "cat"

	implementazione	
Profilo	**Dominio**	**Policy**
urn:sitr:pro:0007-security-admin	ActiveDirectory/Oracle	Il ruolo di gestore della sicurezza deve consentire principalmente di: 1- Gestire accounts su Active Directory 2- Gestire privilegi su Oracle 3- Intervenire sui domini locali Per fare ciò occore quindi: 1- Creare un ruolo (gruppo) su AD che possa amministrare gli account; questo ruolo ovviamente esiste già, di sistema, ed è "Account Operators". **NET GROUP ROLE_IDT_SEC_ADMIN /ADD /DOMAIN** **NET GROUP "Account Operators" ROLE_IDT_SEC_ADMIN /ADD /DOMAIN**[24] **NET GROUP ROLE_IDT_SEC_ADMIN <user1> /ADD /DOMAIN** 2- Creare un ruolo (gruppo) su Oracle che possa amministrare gli utenti ed i ruoli. Tale ruolo di sistema ovviamente esiste già ed è DBA **create role ROLE_IDT_SEC_ADMIN;** **grant DBA to ROLE_IDT_SEC_ADMIN;** **grant ROLE_IDT_SEC_ADMIN to <user1>;** 3- Per intervenire sui domini locali, invece occorre procedere di caso in caso. In particolare: a. Geoserver: l'utente del dominio AD deve poter accedere in modifica ai file appositi contenuti nella cartella di configurazione di Geoserver (geoserver_data_dir). Occorre quindi dare i privilegi di modifica sulla share opportuna[25] **SetACL.exe -on "sitr_app_smb" -ot shr -actn ace -ace "n:SITRS\ROLE_IDT_SEC_ADMIN;p:change"** b. FeatureCatalogue: l'utente del dominio AD deve poter accedere in modifica al file contenuto nella cartella di deploy. **SetACL.exe -on "fc-ejb.jar" -ot file -actn ace -ace "n:SITRS\ROLE_IDT_SEC_ADMIN;p:change"** c. GestoreMetadati: l'utente del dominio Oracle deve poter accedere in modifica alla tabella in cui sono memorizzati gli utenti. **grant INSERT,SELECT,UPDATE,DELETE** **on** **RX_UTENTE** **to** **ROLE_IDT_SEC_ADMIN;** d. Repertorio: l'utente del dominio Repertorio deve essere un amministratore

[24] Il comando in questione non funziona con gruppi innestati, per cui l'operazione va eseguita da console di amministrazione del domain controller; qui è stata indicata per chiarezza.

[25] Non si ritiene necessario utilizzare una granularità più fine, a livello di singoli file interessati dalla configurazione di sicurezza.

	implementazione	
Profilo	**Dominio**	**Policy**
		della sicurezza. Va dunque creato un "profilo" (gruppo di utenti) e ad esso associata la "funzione" per la gestione della sicurezza (che è **sec_h_user**). Ovviamente vanno creati anche gli utenti e associati al profilo. Tutte queste operazioni sono eseguibili solo da GUI. e. ArcSDE: l'utente che dà le grant su una tabella spaziale può essere solo l'utente proprietario; nel nostro caso è l'utente IDT.
urn:sitr:pro:0008-sys-admin	ActiveDirectory	L'utente deve essere nel gruppo Administrator **NET GROUP ROLE_IDT_SYS_ADMIN /ADD /DOMAIN** **NET GROUP "Administrators" ROLE_IDT_SYS_ADMIN /ADD /DOMAIN**[26] **NET GROUP ROLE_IDT_SYS_ADMIN <user1> /ADD /DOMAIN**
urn:sitr:pro:0009-geo-admin	Geoserver	definire gli utenti e i ruoli: nel file GEOSERVER_DATA_DIR/security/user.properties inserire le righe <user>=<psswd>,ROLE_ADMINISTRATOR
	RepositoryManager	Creare un profilo "ROLE_IDT_GEO_ADMIN" Associare al profilo tutte le funzioni tranne quella per la gestione della sicurezza. Associare l'utente al profilo.
urn:sitr:pro:0010-app-md-read	Oracle	Si tratta di assegnare i privilegi di lettura a tutte le tabelle dello schema MD. Si crea il ruolo: **create role ROLE_IDT_APP_MD_READER;** e poi si esegue il risultato della seguente query: **select** **'grant select on ' || table_name || ' to ROLE_IDT_APP_MD_READER;'** **from** **DBA_TABLES** **where** **OWNER = 'MD';**
urn:sitr:pro:0011-app-md-write	Oracle	Si tratta di assegnare i privilegi di scrittura a tutte le tabelle dello schema MD. Si crea il ruolo: **create role ROLE_IDT_APP_MD_WRITER;** e poi si esegue il risultato della seguente query:

[26] Il comando in questione non funziona con gruppi innestati, per cui l'operazione va eseguita da console di amministrazione del domain controller; qui è stata indicata per chiarezza.

	implementazione	
Profilo	**Dominio**	**Policy**
		select 'grant select,insert,update,delete on ' || table_name || ' to ROLE_IDT_APP_MD_WRITER;' from DBA_TABLES where OWNER = 'MD';
urn:sitr:pro:0012-app-fc-read	Oracle	Si tratta di assegnare i privilegi di lettura a tutte le tabelle dello schema FC. Si crea il ruolo: create role ROLE_IDT_APP_FC_READER; e poi si esegue il risultato della seguente query: select 'grant select on ' || table_name || ' to ROLE_IDT_APP_FC_READER;' from DBA_TABLES where OWNER = 'FC';
urn:sitr:pro:0013-app-fc-write	Oracle	Si tratta di assegnare i privilegi di scrittura a tutte le tabelle dello schema FC. Si crea il ruolo: create role ROLE_IDT_APP_FC_WRITER; e poi si esegue il risultato della seguente query: select 'grant select,insert,update,delete on ' || table_name || ' to ROLE_IDT_APP_FC_WRITER;' from DBA_TABLES where OWNER = 'FC';
urn:sitr:pro:0014-free-sde-read	SDE (Oracle)	Attraverso le utilità ArdSDE si associano i privilegi di lettura alle singole tabelle spaziali che costituiscono i vari dataset ad accesso libero. Solo l'utente proprietario (IDT) può lanciare il comando per cui non si possono creare ruoli appositi. Gli utenti a cui vengono concessi i privilegi sono del domini Oracle. sdelayer -o grant -l DBTSEDETRASPORTOFERRO -U ROLE_IDT_DTS02_READER -A SELECT -u IDT -p <passwd> sdelayer -o grant -l DBTACQUEDOTTO -U ROLE_IDT_DTS02_READER -A SELECT -u IDT -p <passwd> … sdelayer -o grant -l DBTVIABILITAMISTASECONDARCHI -U ROLE_IDT_DTS02_READER -A SELECT -u IDT -p <passwd> (… si ripete per i dataset 03-13 …) sdelayer -o grant -l PICCOLIINVASI -U ROLE_IDT_DTS14_READER -A SELECT -u IDT -p <passwd>

	implementazione	
Profilo	**Dominio**	**Policy**
urn:sitr:pro:0015-catasto-sde-read	SDE (Oracle)	Attraverso le utilità ArdSDE si associano i privilegi di lettura alle singole tabelle spaziali che costituiscono il dataset catasto. Solo l'utente proprietario (IDT)può lanciare il comando per cui non si possono creare ruoli appositi. **sdelayer –o grant –l ACQUECATASTO –U ROLE_IDT_DTS01_READER –A SELECT –u IDT –p <passwd>** **sdelayer –o grant –l CAMPITURECATASTO –U ROLE_IDT_DTS01_READER –A SELECT –u IDT –p <passwd>** **…** **sdelayer –o grant –l TESTIPARTICELLECATASTO –U ROLE_IDT_DTS01_READER –A SELECT –u IDT –p <passwd>**
urn:sitr:pro:0051-app-service-exec	Active Directory	Creazione di ruoli (gruppi) e utenti per la esecuzione degli Application Server (Tomcat, JBOSS,…,) gli Application Server dei Map Server, ArcIMS e il Web Server con i privilegi appositi. I gruppi non vengono associati al Built-in group "Remote Desktop" per cui i relativi utenti non possono essere utilizzati per collegarsi ai server. **NET GROUP ROLE_IDT_MAPSERV_EXEC /ADD /DOMAIN** **NET GROUP ROLE_IDT_APPSERV_EXEC /ADD /DOMAIN** **NET GROUP ROLE_IDT_WEBSERV_EXEC /ADD /DOMAIN** **NET GROUP ROLE_IDT_AIMSERV_EXEC /ADD /DOMAIN** **NET GROUP ROLE_IDT_MAPSERV_EXEC <user_tomcat_map> /ADD /DOMAIN** **NET GROUP ROLE_IDT_APPSERV_EXEC <user_tomcat_app> /ADD /DOMAIN** **NET GROUP ROLE_IDT_APPSERV_EXEC <user_jboss> /ADD /DOMAIN** **NET GROUP ROLE_IDT_AIMSERV_EXEC <user_arcims> /ADD /DOMAIN** **NET GROUP ROLE_IDT_WEBSERV_EXEC <user_apache> /ADD /DOMAIN** A tali gruppi si danno i privilegi sulle share di rete necessarie: **SetACL.exe -on "dati" -ot shr -actn ace -ace "n:SITRS\ROLE_IDT_MAPSERV_EXEC;p:full"** **SetACL.exe -on "dati" -ot shr -actn ace -ace "n:SITRS\ROLE_IDT_AIMSERV_EXEC;p:full"** **SetACL.exe -on "geoblog" -ot shr -actn ace -ace "n:SITRS\ROLE_IDT_WEBSERV_EXEC;p:full"** **SetACL.exe -on "geoserver_data_dir" -ot shr -actn ace -ace "n:SITRS\ROLE_IDT_MAPSERV_EXEC;p:full"** **SetACL.exe -on "geowebcache" -ot shr -actn ace -ace "n:SITRS\ROLE_IDT_MAPSERV_EXEC;p:full"** **SetACL.exe -on "scarico" -ot shr -actn ace -ace "n:SITRS\ROLE_IDT_WEBSERV_EXEC;p:full"**

	implementazione	
Profilo	**Dominio**	**Policy**
		SetACL.exe -on "temp_scarico" -ot shr -actn ace -ace "n:SITRS\ROLE_IDT_MAPSERV_EXEC;p:full" SetACL.exe -on "temp_scarico" -ot shr -actn ace -ace "n:SITRS\ROLE_IDT_WEBSERV_EXEC;p:full"
urn:sitr:pro:0052-app-etl-exec	Active Directory	Creazione di ruolo (gruppo) e utenti per la esecuzione degli ETL Il gruppo non viene associato al Built-in group "Remote Desktop" per cui i suoi utenti non possono essere utilizzati per collegarsi ai server. NET GROUP ROLE_IDT_ETL_EXEC /ADD /DOMAIN NET GROUP ROLE_IDT_ETL_EXEC <user_etl_01> /ADD /DOMAIN … NET GROUP ROLE_IDT_ETL_EXEC <user_etl_15> /ADD /DOMAIN SetACL.exe -on "ETL" -ot shr -actn ace -ace "n:SITRS\ROLE_IDT_ETL_EXEC;p:full"
urn:sitr:pro:0101-app-etl-01-writer	Oracle	Si crea un ruolo (anche se vi apparterrà un solo utente) con i provilegi per aggiornare il dataset corrispondnete all'ETL. Questo ruolo viene associale ad un solo utente che sarà utilizzato dall'ETL per scrivere nel DBUnico ed in particolare per le tabelle del proprio dataset. Si crea il ruolo: create role ROLE_IDT_APP_ETL01_WRITER; Si crea l'utente: create user <user_etl01> IDENTIFIED BY <password>; Si associa al ruolo: grant ROLE_IDT_APP_ETL01 to <user_etl_01_w>; Si danno i permessi di lettura su tutte le tabelle dello schema IDT select 'grant SELECT on ' || table_name || ' to ROLE_IDT_APP_ETL01_WRITER;' from DBA_TABLES where OWNER = 'IDT'; Si danno i permessi di scrittura sulle tabelle del dataset. grant INSERT,UPDATE,DELETE on ACQUECATASTO to ROLE_IDT_APP_ETL01_WRITER; grant INSERT,UPDATE,DELETE on CAMPITURECATASTO to ROLE_IDT_APP_ETL01_WRITER; … INSERT,UPDATE,DELETE on TESTIPARTICELLECATASTO to ROLE_IDT_APP_ETL01_WRITER;

	implementazione	
Profilo	**Dominio**	**Policy**
…		

urn:sitr:pro:0114-app-etl-14-writer	Oracle	Si crea un ruolo (anche se vi apparterrà un solo utente) con i provilegi per aggiornare il dataset corrispondnete all'ETL. Questo ruolo viene associale ad un solo utente che sarà utilizzato dall'ETL per scrivere nel DBUnico ed in particolare per le tabelle del proprio dataset.
		
		Si crea il ruolo:
		`create role ROLE_IDT_APP_ETL14_WRITER;`
		
		Si crea l'utente:
		`create user <user_etl14> IDENTIFIED BY <password>;`
		
		Si associa al ruolo:
		`grant ROLE_IDT_APP_ETL14 to <user_etl_14_w>;`
		
		Si danno i permessi di lettura su tutte le tabelle dello schema IDT
		`select`
		`'grant SELECT on ' || table_name || ' to ROLE_IDT_APP_ETL14_WRITER;'`
		`from`
		`DBA_TABLES`
		`where`
		`OWNER = 'IDT';`
		
		Si danno i permessi di scrittura sulle tabelle del dataset.
		
		`grant INSERT,UPDATE,DELETE on PICCOLIINVASI to ROLE_IDT_APP_ETL14_WRITER;`

urn:sitr:pro:0115-app-etl-15-writer	Active Directory	Già realizzato con le policy per l'utente di esecuzione. In questo caso infatti, utente di esecuzione del batch e di collegamento al DB (che è una cartella su file system) coincidono.

Tabella 28 - Implementazione policy

2.9.4. Dipendenze tra policy

Tra le diverse risorse esistono delle relazioni di dipendenza che comportano poi dipendenze tra policy definiti sulle stesse risorse. Se non tenute in giusta considerazione queste dipendenze possono produrre situazioni incongruenti che possono portare anche a malfunzionamenti del sistema. Un esempio di tali dipendenze è la dipendenza che c'è tra la risorsa "GestoreMetadati" (un applicazione) e lo schema Oracle nel quale sono memorizzati gli oggetti di database che utilizza questa applicazione: schema METADATI. In questo caso l'assegnazione di policy riguardanti l'utilizzo dell'applicazione in gestione e la mancata assegnazione di policy relative alla scrittura nel relativo schema dati può portare addirittura a situazioni di errore durante l'utilizzo dell'applicazione (Oracle impedirebbe all'utente di apportare le modifiche ai dati definite attraverso l'utilizzo dell'applicazione e questo risulterebbe in un run-time

error al momento del tentativo di transazione). In altre situazioni l'incongruenza non produrrebbe errori applicativi, ma la politica di autorizzazione risulterebbe poco chiara: immaginiamo un utente che riceva l'autorizzazione ad accedere in modalità diretta (connessione al DB con una client GIS) ad una Feature Type. Chiaramente se tale utente non riceve anche l'autorizzazione ad accedere alla FT tramite WFS questa situazione è chiaramente inconsistente, perché sempre si tratta di accesso al dato.

Sulla base di questi ragionamenti è opportuno evidenziare le dipendenze tra risorse e qualificarle come "forti" o "deboli" sulla base degli effetti che può aver il non tenerle in considerazione al momento di definire le policy relative.

Mentre la tipologia "debole" di dipendenza è più concettuale e indipendente dalla implementazione di applicazioni e/o servizi, per quella "forte" c'è una stretta correlazione: si pensi infatti al caso dell'applicazione di gestione dei metadati e quella di gestione del feature catalogue: se concettualmente la dipendenza tra utilizzo dell'applicazione e diritti sui relativi schemi DB c'è sempre, nel caso del GestoreFeatureCatalogue che è un'applicazione web, l'utente con cui si accede al DB è un utente applicativo e non coincide con quello umano che si logga all'applicazione. L'assenza di diritti di scrittura o lettura sullo schema di DB per l'utente di gestione del feature catalogue non produce quindi alcun problema a livello di funzionalità dell'applicazione.

Esempi di dipendenze tra risorse che producono dipendenze tra policy:

applicazione (servizi) → Schema Oracle / applicazione (servizi) → File

Applicazione che utilizza o gestisce dati su DB o su filesystem. Ad esempio il GestoreFeatureCatalogue gestisce un catalogo implementato su DB. Non consideriamo ricadenti in questo caso i file di configurazione propri dell'applicazione quando questi sono contenuti nel pacchetto di distribuzione e dispiegati assieme al software in ambiente di esecuzione.

layer → Tabelle/viste Oracle / layer → file

Un layer è il prodotto dalla renderizzazione di uno o più dati geografici. I dati sono mantenuti o su tabelle/viste Oracle o su filesystem. Ad esempio: il layer dbu:ALBERIMONUMENTALI è prodotto dalla renderizzazione della tabella Oracle IDT.ALBERIMONUMENTALI.

feature type → tabelle/viste Oracle / feature type → file

Una Feature Type è un dato geografico in formato standard GML, ma è prodotto dalla elaborazione di un dato fisico mantenuto o su tabelle/viste Oracle o su filesystem. Ad esempio: la Feature Type dbu:ALBERIMONUMENTALI è basata sulla tabella Oracle IDT.ALBERIMONUMENTALI.

applicazione → servizi

Un'applicazione può essere basata su un'architettura a servizi e quindi non accedere direttamente allo strato dei dati, ma utilizzare uno strato di servizi che garantiscono una maggiore riutilizzazione del software e interoperabilità. Ad esempio la ConsultazioneCatalogoDati si basa sul servizio MetadatiISO per accedere alla banca dati dei metadati.

Tabelle SDE → Tabelle Oracle

Una tabella spaziale SDE non esiste se non esiste la tabella Oracle corrispondente.

A questo proposito l'Amministrazione ritiene opportuno adottare come standard di gestione della IDT la creazione del layer ArcSDE corrispondente ogni qualvolta si crea una tabella spaziale Oracle e di concedere sugli oggetti corrispondenti i medesimi privilegi agli utenti autorizzati all'accesso.

risorsa	risorsa dipendente	tipo dipendenza
urn:sitr:res:dbs:0002-md	urn:sitr:res:app-0001-GestoreMetadati	forte
urn:sitr:res:dbs:0005-fc	urn:sitr:res:app-0002-GestoreFeatureCatalogue	debole
urn:sitr:res:app-0012-FeatureCatalogue	urn:sitr:res:app-0002-GestoreFeatureCatalogue	debole
urn:sitr:res:app-0003-CatalogoDati	urn:sitr:res:app-0001-GestoreMetadati	debole

urn:sitr:res:dbo-0001-DBTSEDETRASPORTOFERRO	urn:sitr:res:ftc-0001-DBTSEDETRASPORTOFERRO	debole
…	…	…
urn:sitr:res:dbo-0191-TESTIPARTICELLECATASTO	urn:sitr:res:ftc-0191-TESTIPARTICELLECATASTO	debole
urn:sitr:res:dbo-0001-DBTSEDETRASPORTOFERRO	urn:sitr:res:sde-0001-DBTSEDETRASPORTOFERRO	forte
…	…	...
urn:sitr:res:dbo-0191-TESTIPARTICELLECATASTO	urn:sitr:res:sde-0191-TESTIPARTICELLECATASTO	forte
urn:sitr:res:fso-0001-ORTOFOTOIT2000	urn:sitr:res:ftc-1001-ORTOFOTOIT2000	debole
…	…	…
urn:sitr:res:fso-0004-CTR10K	urn:sitr:res:ftc-1004-CTR10K	debole
urn:sitr:res:ftc-0001-DBTSEDETRASPORTOFERRO	urn:sitr:res:lyr-0001-DBTSEDETRASPORTOFERRO	debole
…	…	...
urn:sitr:res:ftc-1004-CTR10K	urn:sitr:res:lyr-1004-CTR10K	debole
urn:sitr:res:srv-0009-MetadatiISO	urn:sitr:res:app-0003-CatalogoDati	forte
urn:sitr:res:srv-0012-RicercaToponimi	urn:sitr:res:app-0048-RicercaToponimi	forte

Tabella 29 - Dipendenze tra risorse

3. Gestione delle Autorizzazioni

L'aspetto autorizzativo del sistema di sicurezza del SITR è qui affrontato dal solo punto di vista di modellazione dei dati interessati da questo componente trascurando al momento tutti i problemi di gestione vera e propria.

3.1. Modellazione concettuale/logica delle autorizzazioni

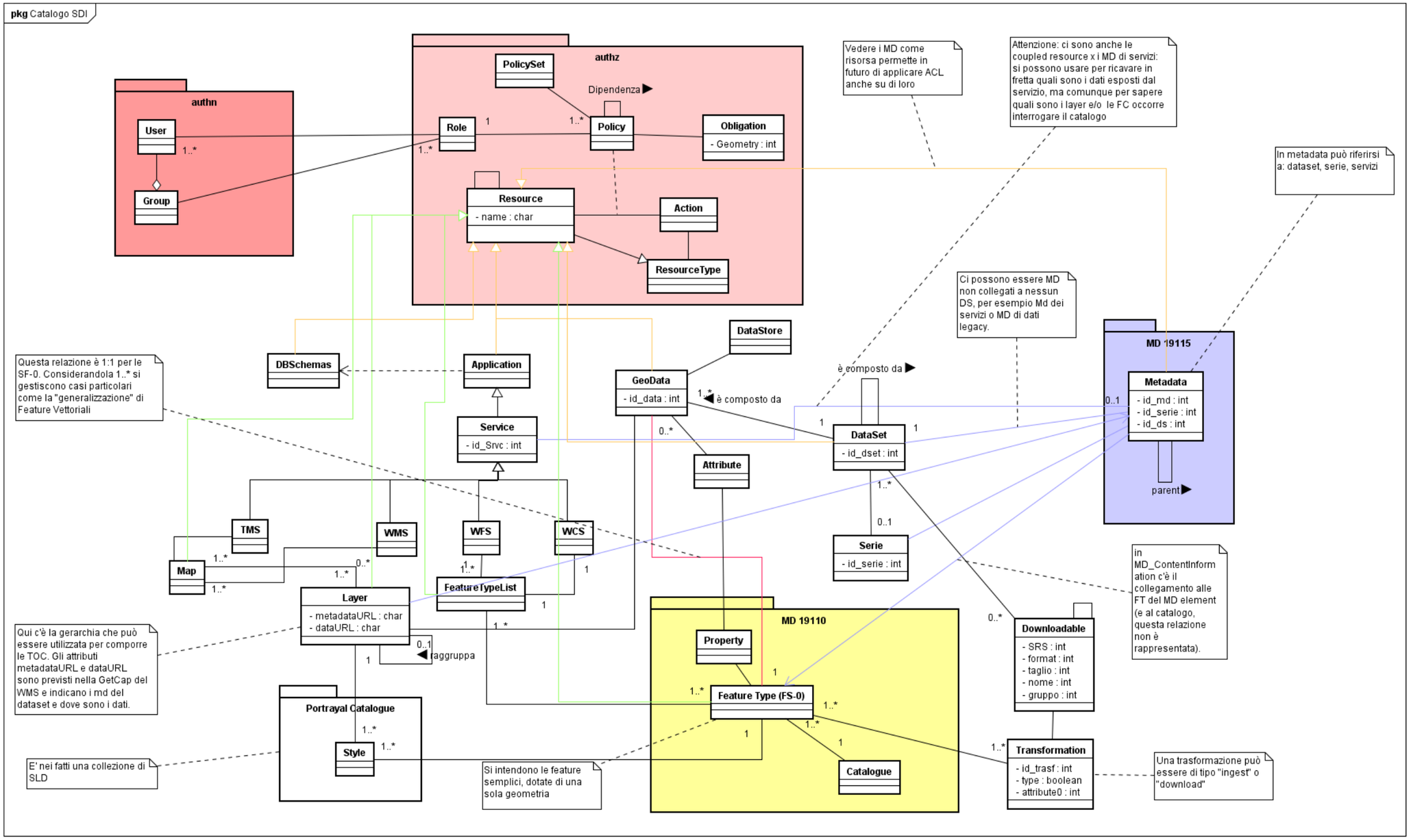


Figura 1 - Modellazione concettuale autorizzazioni

Il modello riportato in Figura 1 esprime questi concetti:

Action = Tutte le possibile azioni eseguibili su una data risorsa e sui cui è possibile esercitare un controllo.

Application = Applicazione

Catalogue **=** Collezione di FeatureType e relative metadati ISO 19110

Dataset = Insieme di dati geografici individuabile in maniera univoca mediante caratteristiche distintive

DBSchemas **=** Schema Oracle

Downloadable **=** Pacchetto di dati geografici in un formato trasferibile mediante FTP o download HTTP.

FeatureType = Rappresentazione di un fenomeno del mondo reale secondo uno specifico modello; è dotata di attributi geometrici. Nel nostro caso effettuiamo una semplificazione prendendo in considerazione solo le Simple Feature di profilo 0 (SF-0) ovvero quelle feature i cui attributi non sono altre feature e che si possono mappare con una tabella di database o con un XML "piatto", non strutturato. Un'ulteriore semplificazione che imponiamo è sul numero degli attributi geometrici.

FeatureTypeList = Insieme di FeatureType servite da un medesimo WFS

GeoData **=** Oggetto fisico digitale che implementa il dato geografico **Obligation =** particolare limitazione o vincolo associato ad una policy; limita l'azione sulla base di valori di alcuni attributi che caratterizzano la risorsa stessa o l'azione come il tempo o le coordinate spaziali.

Layer **=** Rappresentazione di dati geografici ad uso dell'uomo; è l'unità minima di una mappa.

Map = Insieme di layer servito da un medesimo WMS

Metadata **=** Insieme di informazioni su dataset geografici e/o servizi.

Policy = E' una coppia costituita da azione e risorsa e indica un privilegio assegnabile ad un utente.

PolicySet = Insieme di policy raggruppabili per caratteristiche comuni delle policy stesse.

Resource = Risorsa da assoggettare a controllo degli accessi

ResourceType = Tipologia di risorsa

Role = Insieme di policy da assegnare agli utenti; il raggruppamento è fatto sulla basa dei destinatari.

Service = Servizio web sia SOAP che REST.

Transformation = Trasformazione di dati geografici

TMS = Tiled Map Service

User = Utente del sistema

WCS = Web Coverage Service

WFS = Web Feature Service

WMS = Web Map Service

E queste relazioni:

Una **Resource** può essere costituita da un'**Application**, un **Layer**, una **Map**, una **FeatureType**, una **FeatureTypeList**, un **Metadata** o un **Downloadable**.

Un specializzazione di un'**Application** è un **Service**.

Un **Service** può essere un **WMS**, un **WFS**, un **WCS** o un **TMS**.

Una **Map** è formata da **Layer**. I **Layer** possono essere raggruppati a loro volta in maniera gerarchica. Un **Layer** è la rappresentazione di una o più **FeatureType**.

Una **Map** è servita da uno o più **WMS** (o **TMS**) mentre un **WMS** (**TMS**) server una sola **Map**.

Una **FeatureTypeList** è un insieme di FeatureType; un **WFS** o (**WCS**) serve una sola **FeatureTypeList** mentre una FeatureTypeList può essere servita da più **WFS** (o **WCS**).

Una **FeatureType** è fisicamente rappresentata da uno o più **GeoData** (la molteplicità serve a rappresentare particolari situazioni come le "Feature pregeneralizzate", ma la relazione largamente rispetta la cardinalità 1:1). Una **FeatureType** è catalogata all'interno di un solo **Catalogue** che viceversa ne descrive molteplici.

I **GeoData** possono essere raggruppati in **DataSet**. Un **Metadata** descrive un **DataSet** (che può collassare in un singolo **GeoData**) oppure un **Service**. I **DataSet** possono combinarsi a loro volta in varie aggregazioni. Particolari raggruppamenti di **DataSet** sono costituite dalle **Series**. Un **DataSet** può appartenere ad una sola **Series**. Un **Metadata** può riferirsi anche ad una **Series,** ma non ad altri tipi di raggruppamenti di **DataSet**.

Un **Metadata** può contenere un riferimento alle **FeatureType** (e al relativo **Catalogue**) che compongono il **DataSet** che descrive.

I **Metadata** hanno una relazione fra di loro stessi dovuta alla necessità (dettata da normative) di gestire la loro storicizzazione. Un **Metadata** può avere quindi un genitore e/o un figlio: questa relazione descrive una catena lineare di versioni successive del **Metadata**.

Un **Layer** nasce dall'operazione di rappresentazione (o, con un anglicismo, "renderizzazione", o più correttamente "portrayal" ovvero trasformazione del dato in un'immagine interpretabile dall'uomo) di una o più **Feature Type** applicando regole e simbologie definite in uno **Style**[27]. Più **Style** possono

[27] Uno Style è descritto in maniera standard da un documento XML detto SLD, Styled Layer Descriptor. SLD è una specifica OGC.

essere definiti per trasformare le medesime **Feature Type** in **Layer** differenti. Questa relazione quindi è una relazione n:m dove lo **Style** può essere modellato anche come entità associativa.

Avere a disposizioni più Style per ciascun layer produce di fatto una moltiplicazione dei Layer a disposizione dei client; nello stesso tempo si viene a creare nella IDT un catalogo di stili, o **Portrayal Catalogue**, che ne aumenta la complessità di gestione (nella IDT Geoserver ne implementa uno molto rudimentale, interrogabile in maniera indiretta tramite il servizio WMS). Al momento si considera un solo **Style** per **Layer** (il default Style, che non deve nemmeno essere specificato nelle richieste): quindi nell'architettura della IDT i **Layer** sono da considerare come **Layer** associati al default **Style**.

Un **Layer** può indicare (attraverso la descrizione fornita dal **WMS** che lo serve) quale **Metadata** lo descrive indirettamente descrivendo il **DataSet** che implementa le **FeatureType** che producono il **Layer** stesso. Allo stesso modo un **Layer** può avere riferimenti ai **GeoData** sottostanti.

Una **Resource** è caratterizzata da tutte le possibili **Action** esercitabili su di essa. Una particolare istanza della relazione **Resource-Action** costituisce una **Policy** e questa è caratterizzata eventualmente da una o più **Obligation**.

Le **Policy** possono avere delle dipendenze fra loro, derivanti dalle dipendenze tra **Resource**.

3.2. Implementazione schema autorizzazioni (RDBMS)

Vedi DB Access allegato.

4. Interventi sul sistema

In questo capitolo vengono esaminate alcune attività da eseguire sul sistema al fine da avvicinarsi alla situazione teorica di un unico sistema di autenticazione/autorizzazione basato su un unico user repository ed integrata con tutte le applicazioni e servizi.

4.1. Unificazione directory utenti di Oracle e di rete Windows

Riuscire ad utilizzare in Oracle un repository di utenti esterno a proprio ed in special modo quello della directory LDAP è un passo fondamentale della messa in sicurezza della IDT.

Oracle prevede 4 tipi di autenticazione possibili:

- Database
- External
- Global
- Proxy

DATABASE
La prima è quella che normalmente si utilizza e anche nel caso particolare della IDT del SITR è quella attualmente in uso. Gli utenti e le relative password sono gestite interamente dal DB.
Il comando per creare un utente autenticato dal DB è il seguente:

```
CREATE USER <user_name> IDENTIFIED BY <password>;
```

EXTERNAL
L'autenticazione esterna è una configurazione che lascia ad Oracle il compito di gestire gli utenti, ma le relative password e il processo di autenticazione è demandato ad soggetto terzo.
In particolare possiamo avere due tipologie differenti di autenticazione esterna:

- Effettuata dal sistema operativo
- Effettuata da un servizio di rete

In entrambi i casi utenti con autenticazione esterna possono convivere con utenti con autenticazione da database.
Il comando per la creazione di un utente autenticato esternamente è:

```
CREATE USER <user_name> IDENTIFIED EXTERNALLY;
```

Nel caso di autenticazione da **Sistema Operativo**, occorre considerare due grosse categorie di scenari: quella in cui il server è configurato in modalità SHARED e quella DEDICATED. La prima modalità permette di utilizzare uno stesso processo sul server per molteplici connessione sul client, producendo

un risparmio notevole di risorse, perché in alternativo ad ogni connessione client corrisponde un unico processo sul server. Questa modalità comporta però l'utilizzo di Oracle Net Service per stabilire la connessione con il server SHARED, e questo tipo di connessione è considerata NON SICURA.
L'autenticazione esterna da Sistema Operativo è abilitata solo su connessione sicura per cui esiste un parametro da settare eventualmente sul server per ovviare a questo problema:

```
REMOTE_OS_AUTHEN = TRUE
```

Questa configurazione, però, espone il DB ad una grossa vulnerabilità, perché sui client è possibile facilmente bypassare l'autenticazione del Sistema Operativo, creando ad esempio o degli utenti locali o degli utenti di macchine virtuali che simulano in tutto o in parte il nome degli utenti registrati su Oracle. In questo modo con un utente creato su una macchina virtuale con il nome uguale ad un utente del dominio, verrebbe erroneamente riconosciuto da Oracle (che non effettua alcun controllo se non il match del nome utente con quelli definiti al suo interno) come un utente autenticato esternamente.

Questa digressione (nello scenario del SITR il server è configurato in modalità DEDICATED per cui non sarebbe necessario disattivare il controllo per l'autenticazione esterna su connessione sicura) è stata fatta poiché la configurazione in questione è l'unica che consente di attivare l'autenticazione esterna nel caso di un server Oracle in ambiente Linux e di client costituiti da workstation Windows all'interno di un dominio di rete Windows Active Directory, quale presenta l'architettura del SITR (vedi test autenticazione esterna da Sistema Operativo illustrati successivamente).

Nel caso di autenticazione attraverso un **servizio di rete**, occorre attivare la Oracle Advanced Security (OAS), un'opzione aggiuntiva rispetto la normale configurazione; opzione che caratterizzata anche da un costo di licenza. Qualora si faccia uso di questa modalità, il livello di sicurezza che si ottiene è molto elevato e soddisfa pienamente i nostri requisiti. I servizi di autenticazione di rete supportati sono:

- Kerberos
- Radius
- DCE
- SSL (con certificati digitali)
- PKI (Entrust)

Il primo, Kerberos, è quello più indicato visto che Microsoft Active Directory di Windows 2003 Server implementa tale protocollo e di fatto AD può essere visto a tutti gli effetti come un KDC (Key Distribution Center) di un sistema Kerberos.

Questa soluzione, inoltre, consente di integrare anche scenari di reti ibride (Linux + Windows) come quello del SITR.

GLOBAL
Questo tipo di autenticazione permette di esternalizzare non solo la gestione delle password, ma anche quella degli utenti (ed i ruoli). In pratica è possibile definire su una directory LDAP-compliant gli utenti

e disaccoppiarli dagli schemi del DB e fare in modo che condividano con gli opportuni diritti lo stesso schema. L'autenticazione è basata su SSL o sulla Windows NT nativa.
Tale soluzione, sebbene sia indicata per un generica directory LDAP, è garantita con Oracle Internet Directory, soluzione proprietaria di Oracle che oltre a fornire servizi LDAP offre anche servizi di sincronizzazione e replicazione per realizzare un'unica directory virtuale verso altri user repository come anche Microsoft AD.

PROXY
Si tratta di sviluppare un software di autenticazione che funga da middle tier tra Oracle e il client.
Il software in questione si connette al DB al posto del client, agendo così come un proxy del client stesso.

4.1.1. Autenticazione Oracle esterna mediante servizio di rete Kerberos

Esploriamo in questo paragrafo lo scenario in cui si attiva l'autenticazione esterna di Oracle basandosi su un servizio di rete Kerberos offerto dal domain controller della rete Windows.

4.1.1.1. Kerberos

Kerberos è un protocollo di rete per l'autenticazione che permette l'utilizzo sicuro, mediante mutua identificazione, di servizi di rete da parte di client che costituiscono entrambi nodi di una rete non sicura.
Kerberos si basa fortemente sul concetto di **crittografia a chiave simmetrica**, ovvero algoritmi di crittazione reversibili mediante l'uso della medesima chiave di crittazione o di una chiave derivata con una semplice trasformazione. La **crittografia a chiave simmetrica** è fondata quindi su quello che si chiama un **segreto condiviso** tra le parti che devono scambiarsi messaggi privati, segreto che deve essere trasmesso con modalità esterne al protocollo.
Altro concetto fondamentale del protocollo è la presenza di una terza parte che è ritenuta affidabile da tutti i componenti della rete: questa terza parte è il servizio di autenticazione del sistema Kerberos.

In una rete protetta con il protocollo Kerberos non solo gli utenti sono identificati, ma anche i servizi; ciascun utente e servizio conosce la propria password (il segreto condiviso) e il servizio di autenticazione conosce le password di tutti e le mantiene in un database centrale e unico.

Una volta che un client si autentica verso il servizio di autenticazione, per poter utilizzare un servizio della rete, ad esso non viene ovviamente fornita la password del servizio, ma un **ticket** che è una stringa che contiene il nome dell'utente crittografato dal servizio di autenticazione mediante la password del servizio target (assieme ad altre informazioni come indirizzo IP del client, timestamp e durata del ticket, nome del servizio target). Usando questo ticket nella richiesta al servizio target, quest'ultimo ricava, decrittando con la propria password il ticket stesso, il nome dell'utente e può decidere così se concedere l'accesso oppure no (le altre informazioni rafforzano la sicurezza controllando ad esempio che la richiesta avvenga dallo stesso IP che ha richiesto il ticket, oppure verificando che il ticket non sia scaduto; il nome del servizio è garanzia che l'operazione di decrittazione è avvenuta correttamente).

In realtà, per evitare che tutte le volte che un client vuole utilizzare un servizio di rete debba richiedere un ticket (e che l'utente debba quindi digitare la propria password più volte), il protocollo prevede che il servizio di autenticazione rilasci un **ticket-granting ticket** ovvero un ticket non valido per un particolare servizio target, ma per una servizio di ticket-granting, cioè un servizio che rilascia il ticket per il servizio finale sulla base di un ticket piuttosto che la password di identificazione. In questo modo, data la riusabilità del **ticket-granting ticket**, non è necessario identificarsi più volte con Kerberos per usare diversi servizi.
Il protocollo prevede inoltre che la password non viaggi sulla rete: infatti il ticket-granting ticket viene rilasciato usando la password dell'utente mantenuta nel DB centrale e quella digitata dall'utente viene utilizzata localmente per decrittare il ticket-granting ticket. Se la decrittazione avviene correttamente, allora l'utente è autenticato, altrimenti no.

Il protocollo è reso ancor più sicuro mediante l'utilizzo di chiavi di sessione da usare per la crittazione delle singole comunicazioni. Nella Figura 2 è illustrato un esempio di utilizzo di un servizio C da parte di un utente X.

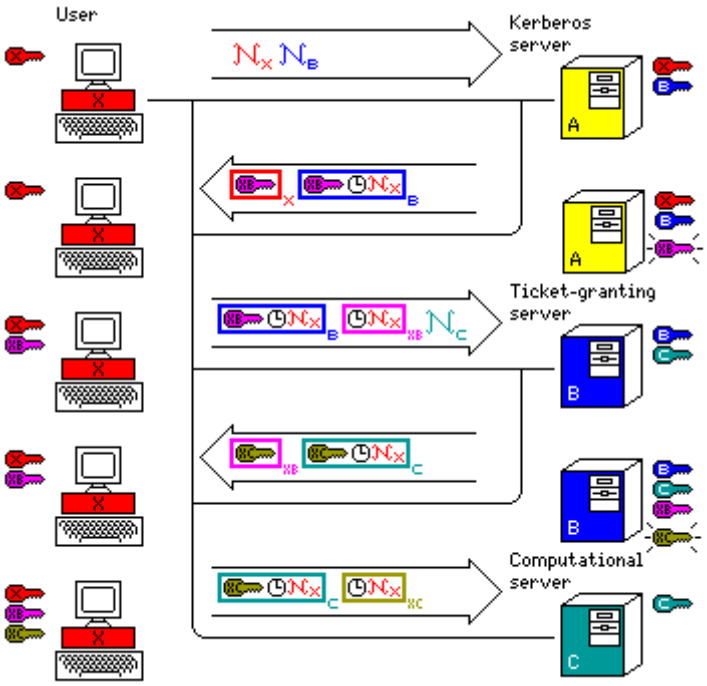


Figura 2 - Autenticazione con Kerberos

1- L'utente ***X*** manda una richiesta al server di autenticazione ***A*** che mantiene permanentemente le chiavi segrete di tutti gli utenti e del servizio di ticket-granting (***B***). Nella richiesta, in chiaro, sono presenti il nome dell'utente N_x e quello del servizio di ticket-granting N_B.
2- Il servizio di autenticazione ***A*** crea una session key per la comunicazione tra l'utente X e il servizio di ticket-granting B. Questa chiave (mostrata in viola in figura) viene crittata con la chiave segreta dell'utente (è mostrata dentro una scatola rossa con il pedice X). Nella risposta è compreso anche il

ticket rappresentato dalla scatola blu con il pedice B: è la crittazione mediante la chiave segreta di B della session key, un time stamp e il nome dell'utente X.

3- L'utente quindi presenta al ticket-granting server una richiesta composta da:
   - Il ticket precedentemente ricevuto dal server di autenticazione
   - L'authenticator, ovvero la crittazione mediante session key del proprio nome e di un time stamp (la scatola viola con pedice XB).
   - Il nome del servizio che intende usare N_c trasmesso in chiaro.

4- Il ticket-granting server B può decrittare il ticket utilizzando la propria chiave segreta e da questa operazione ricava la session key. Con quest'ultima può verificare l'authenticator. Il server B conosce le chiavi segrete di tutti i servizi registrati sulla rete, in particolare quella del servizio C. A questo punto il ticket-granting server B ripete le operazioni fatte precedentemente dal server di autenticazione: genera una session key per la futura comunicazione tra X e C e la cripta con la session key XB; produce inoltre un ticket criptato con la chiave del servizio C (mostrato con una scatola verde con il pedice C) contenente la session key, un time stamp e il nome dell'utente X.

5- Infine l'utente X presenta al servizio che vuole utilizzare C:
   - Il ticket precedentemente ricevuto dal ticket-granting server
   - L'authenticator, ovvero la crittazione mediante session key del proprio nome e di un time stamp (la scatola verde con pedice XC).

GLOSSARIO

KDC = Key Distribution Center. Consiste di tre componenti logiche: il database di tutti i principal e le loro chiavi segrete, l'Authentication Server e il Ticket Granting Server. Normalmente queste tre componenti sono integrate in un unico programma. In ogni realm deve esserci almeno un KDC.

Keytab = E' un file che contiene una o più chiavi. Un host o un servizio usano un keytab file più o meno allo stesso modo in cui un utente usa la propria password.

Principal = Ogni entità contenuta in un'installazione Kerberos, inclusi utenti, computer, servizi, stampanti … ha un principal associata ad essa. I principal sono nomi univoci globali. Per garantire questa unicità i nomi dei principal sono organizzati gerarchicamente.Ogni principal inizia con uno user name o un service name chiamato **primary**, seguiti da una **instance** opzionale. Quest'ultima ha due significati diversi per service principal o user principal. La sintassi quindi è **primary/instance@REALM**

Realm = la rete logicamente servita da un singolo database Kerberos. Per convenzione i nomi dei realm sono solitamente in maiuscolo per differenziarli dal dominio internet.

4.1.1.2. Active Directory, Kerberos e Oracle

Active Directory si basa anche sul protocollo Kerberos v.5 e implementa un KDC compliant con le specifiche MIT. Oltre a ciò viene supportata l'interoperabilità con client Kerberos Linux (è possibile anche integrare un realm Kerberos Linux con AD, ma non è il caso che interessa a noi). Infatti lo

scenario che vogliamo esplorare è quello in cui in un unico realm gestito dal KDC di Windows Server 2003 dove il server Oracle costituisce un servizio protetto dal protocollo Kerberos.
Tale possibilità è offerta dalla Oracle Advanced Security Option (ASO), che offre la possibilità di esternalizzare la gestione dell'autenticazione in base a diversi possibili schemi, di cui Kerberos è uno dei supportati. Il collegamento con AD può essere anche configurato a livello di LDAP (altro protocollo standard supportato da AD), ma, a parte la necessità di estendere lo schema LDAP, questa modalità risulta di difficile implementazione nel caso in cui il server Oracle è un server Linux.
L'autenticazione LDAP è comunque meno "robusta" di quella Kerberos, dove –ad esempio- le password degli utenti non viaggiano mai sulla rete.

4.1.1.3. TEST: Configurazione di Oracle come servizio protetto da Kerberos

Per il test seguente abbiamo utilizzato una topologia di rete come la seguente:

Server Kerberos (KDC)
Visto che il test non comporta nulla sul domain controller se non la creazione di utenti, si è scelto come KDC il domain controller di produzione.

Host name = dc1sitrs.sitrs.regione.sardegna.net
Domain AD = sitrs.regione.sardegna.net
Kerberos Realm = SITRS.REGIONE.SARDEGNA.NET
SO = WINDOWS SERVER 2003 SP1

Client Kerberos
E' stata usata una macchina virtuale sulla quale è installato Oracle DBMS con la ASO. Il nome del servizio di database sul server Oracle è "IDT".

Host name = vmoracle.sitrs.regione.sardegna.net
Domain AD = sitrs.regione.sardegna.net
Oracle = v.10.2.0.4
SO = Linux

Oracle Client
E' la macchina da cui si stabilisce una connessione al server Oracle. E' stata usata una macchina Windows server 2003

Host name = ?.sitrs.regione.sardegna.net
Domain AD = sitrs.regione.sardegna.net
SO = WINDOWS SERVER 2003 SP?

Su ogni nodo di una rete Kerberos deve esistere un file di configurazione che si chiama **krb5.conf.** Tale file contiene diverse sezioni e le principali sono:

[libdefaults] = definisce tutti i default di configurazione: il dominio di default, la durata di default del ticket,…
[realms] = indica il kdc (kerberos domain controller) ovvero il server di autenticazione per ciascun dominio configurato
[domain_realm] = mappa i domini DNS ai domini kerberos (normalmente i domini kerberos sono gli stessi in lettere maiuscole, ma qui si può esplicitare la corrispondenza nel caso non si usi la convenzione)

Normalmente il principal che identifica il servizio Oracle ha questa forma:

kservice/kinstance@REALM

dove

keyservice = stringa che rappresenta il servizio Oracle; per semplicità si può far coincidere con il database service name.
keyistance = il nome completamente qualificato del server su cui gira il servizio di database
REALM = il nome del dominio a cui appartiene il DB (sempre in maiuscolo)

Vediamo ora le operazioni di configurazione:

1. Registrazione del servizio Oracle in Active Directory
Questo passo crea un identificativo univoco per il servizio di database Oracle (principal) e produce la chiave segreta che sarà condivisa dal server Kerberos e il servizio stesso. Essendo Oracle installato su piattaforma Linux e quindi un servizio non-Windows Server 2003, occorre usare una utility particolare (**ktpass**) che registra il principal e la password del servizio in AD e genera un file contenente la chiave segreta del servizio stesso da memorizzare sul server Oracle. Questo file è un file "keytab" in stile MIT. Sul domain controller, quindi:

- creare un utente <oracle_user>
- Lanciare quindi il comando

```
ktpass –princ IDT/vmoracle.sitrs.regione.sardegna.net@SITRS.REGIONE.SARDEGNA.NET
-mapuser <oracle_user> -pass <oracle_psswd> -DesOnly –crypto des-cbc-crc –ptype
KRB5_NT_PRINCIPAL –out c:\keytab.<oracle_user>
```

NOTE
La versione di Oracle (10.2.0.4) installata presso il SITR supporta solo l'algoritmo di crittazione `DES-CBC-CRC` e `DES_CBC_MD5` e non quello di default di AD (RC4-HMAC) per cui occorre specificare il parametro –crypto scegliendo uno dei due.

Non bisogna flaggare l'opzione che obbliga l'utente a cambiare password al primo login visto che in questo caso si tratta di un utente applicativo.

2. Registrazione dell'utente fruitore del servizio Oracle in Active Directory
Creare l'utente <client_user> in AD.

3. Creazione dell'utente Oracle nel DBMS

```
CREATE USER <client_user> IDENTIFIED EXTERNALLY AS
'<client_user>@SITRS.REGIONE.SARDEGNA.NET';

GRANT CONNECT TO <client_user>@SITRS.REGIONE.SARDEGNA.NET;
```

NOTA: Verificare che sia applicata la patch 5629724 **(Add support for mapping of > 30 character kerberos principal to DB schema) che fa superare il limite di 30 caratteri per gli utenti la cui sicurezza è gestita esternalmente (il nome di un utente esterno comprende anche il suffisso di dominio per cui solitamente è molto lungo).**

4. Configurazione del server Oracle (client Kerberos)

Copiare sia il file keytab.<oracle_user> su una cartella sul server Oracle che il file di configurazione di Kerberos krb5.conf con i parametri seguenti:

```
[libdefaults]
default_realm = SITRS.REGIONE.SARDEGNA.NET

[realms]
SITRS.REGIONE.SARDEGNA.NET = {
kdc = DC1SITRS.SITRS.REGIONE.SARDEGNA.NET
}

[domain_realm]
.sitrs.regione.sardegna.net = SITRS.REGIONE.SARDEGNA.NET
sitrs.regione.sardegna.net = SITRS.REGIONE.SARDEGNA.NET
```

Ipotizziamo di creare un cartella M:\krb5 dove copiare questi file.

Modifichiamo poi il file $ORACLE_HOME/network/admin/sqlnet.ora come mostrato di seguito:

```
SQLNET.KERBEROS5_CONF = M:\Krb5\krb5.conf
SQLNET.KERBEROS5_CONF_MIT = TRUE
SQLNET.AUTHENTICATION_SERVICES = (BEQ,KERBEROS5)
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = SITRS
SQLNET.KERBEROS5_CC_NAME = M:\Krb5\krbcache
SQLNET.KERBEROS5_KEYTAB = M:\Krb5\keytab.<user_oracle>
SQLNET.ENCRYPTION_TYPES_SERVER = (DES)
SQLNET.AUTHENTICATION_REQUIRED=TRUE
```

Dove:

```
SQLNET.KERBEROS5_CONF_MIT specifica se la sintassi del file di configurazione è
quella nuova MIT oppure no
SQLNET.AUTHENTICATION_SERVICES specifica il metodo di autenticazione
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE il nome del servizio Oracle
```

```
SQLNET.KERBEROS5_CC_NAME il nome assoluto del file di cache delle credenziali
SQLNET.KERBEROS5_KEYTAB il nome assoluto del file contenente le chiave segreta
SQLNET.ENCRYPTION_TYPES_SERVER lista di algoritmi accettati per la crittazione
SQLNET.AUTHENTICATION_REQUIRED abilita l'autenticazione esterna
```

5. Configurazione del client

Anche nel client va inserito il file di configurazione krb5.conf con i medesimi parametri del server.
Anche sul client occorre inoltre modificare il file $ORACLE_HOME/network/admin/sqlnet.ora inserendo le seguenti configurazioni:

```
SQLNET.KERBEROS5_CONF = M:\Krb5\krb5.conf
SQLNET.KERBEROS5_CONF_MIT = TRUE
SQLNET.AUTHENTICATION_SERVICES = (KERBEROS5)
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = SITRS

SQLNET.KERBEROS5_CC_NAME = M:\Krb5\krbcache
SQLNET.KERBEROS5_KEYTAB = M:\Krb5\keytab.p
SQLNET.ENCRYPTION_TYPES_CLIENT = (DES)
SQLNET.AUTHENTICATION_REQUIRED=TRUE
```

Il file $ORACLE_HOME/network/admin/tnanames.ora deve contenere i seguenti parametri per connettersi al database. Meglio specificare una connessione di tipo DEDICATED:

```
SITRS =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)
                 (HOST = vmoracle.SITRS.REGIONE.SARDEGNA.NET)
                 (PORT = 1521)
       )
     )
    (CONNECT_DATA = (SERVICE_NAME = sitrs)
                    (SERVER = DEDICATED)
    )
  )
```

6. Autenticazione e connessione a Oracle

Prima di effettuare una connessione al server Oracle occorre richiedere un TGT (Ticket-Granting Ticket) al KDC. Questa operazione si effettua tramite l'utility Oracle okinit specificando l'utente per cui si richiede il ticket.

>okinit <utente_oracle>

L'utility richiede di digitare la password che, ricordiamo, non viene inviata al KDC, ma viene utilizzata per decrittare il messaggio restituito dal KDC. Il ticket viene memorizzato all'interno del file di cache del client di cui, attraverso l'uso del comando oklist, si può vedere il contenuto.
Lanciando il comando a questo punto si dovrebbe constatare la presenza del solo TGT e verificarne la scadenza temporale.

```
Ticket cache: c:\Krb5\krbcache
Default principal: u@SITRS.REGIONE.SARDEGNA.NET

  Valid Starting        Expires          Principal
01-Mar-2010             14:16:19                          01-Mar-2010             22:16:12
krbtgt/SITRS.REGIONE.SARDEGNA.NET@SITRS.REGIONE.SARDEGNA.NET
```

A questo punto si può richiedere la connessione al server Oracle attraverso il comando sqlplus senza specificare né utente né password. La sintassi è la seguente:

> sqlplus /@SITRS

Dove si è specificato il carattere "/" che indica al client Oracle di utilizzare il TGT per ottenere il ticket di autenticazione.
Lanciando a questo punto il comando oklist, oltre al TGT comparirà anche il ticket rilasciato dal servizio Oracle.

```
Ticket cache: c:\Krb5\krbcache
Default principal: U@SITRS.REGIONE.SARDEGNA.NET

  Valid Starting        Expires          Principal
01-Mar-2010             13:26:23                          01-Mar-2010             21:26:20
krbtgt/SITRS.REGIONE.SARDEGNA.NET@SITRS.REGIONE.SARDEGNA.NET
01-Mar-2010             13:27:05                          01-Mar-2010             21:26:20
SITRS/vmoracle.sitrs.regione.sardegna.net@SITRS.REGIONE.SARDEGNA.NET
```

Dopo avere effettuato la disconnessione al servizio Oracle è opportuno rilasciare il ticket utilizzando il comando okdstry.

4.1.2. Autenticazione Oracle esterna mediante SO (ambiente Windows)

Scopo di questa attività è quella di utilizzare l'autenticazione esterna da SO. Per fare questo è necessario però passare ad un ambiente Windows per il server Oracle. Nel test seguente è stato usato un server windows creato su una macchina virtuale.

4.1.2.1. TEST: autenticazione esterna Oracle in Windows

Con questo test si cercano eventuali problemi nella configurazione che vede il DB Server in ambiente Windows impostato per gestire l'autenticazione esterna degli utenti. In particolare si è verificato la possibilità di autenticare utenti appartenenti ai due domini Windows in trust fra di loro "UFFICIOPIANO" e SITRS". Rimangono a tutti gli effetti i problemi di sicurezza evidenziati nel paragrafo precedente.

Per il test si sono utilizzate 3 macchine virtuali:

VMRESTOREORACLEWINDOWS, IP X.X.X.X
Server Oracle 10.2.0.2, istanza DB "SITRS", dominio Windows "SITRS", Windows 2003 Server SP1

VMWINXP_DOMINIO_UFFPIANO, IP X.X.X.X
Client Oracle, dominio Windows "UFFICIOPIANO", Windows XP

VMWINXP_DOMINIO_SITRS, IP X.X.X.X
Client Oracle, dominio Windows "SITRS", Windows XP

La configurazione del client Oracle prevede il settaggio del parametro

```
sqlnet.authentication_services = (NTS)
```

che specifica di utilizzare l'autenticazione nativa di Windows NT.

4.1.3. Autenticazione Oracle esterna mediante SO (ambiente ibrido)

I test effettuati in un ambiente con SO ibridi, ovvero Linux per il database server e ovviamente Windows per il Domain Controller, non hanno portato ad esiti positivi.
Gli utenti non vengono riconosciuti dal DB per via della qualificazione di dominio.

4.2. Installazione Geoserver su HTTPS

La necessità di configurare Geoserver in HTTPS deriva dalla vulnerabilità che affligge la Basic HTTP Authentication, ovvero la trasmissione dei credenziali di autenticazione praticamente in chiaro (solo con una codifica Base64 per evitare problemi di encoding).

HTTPS elimina questo problema di sicurezza (noto come man-in-the-middle-attack) stabilendo un canale criptato tra client e server (mediante protocollo SSL/TLS che viene applicato a livello di trasporto) attraverso il quale avviene la normale comunicazione in protocollo HTTP (che è il protocollo del livello applicativo soprastante).o

Il meccanismo su cui si base HTTPS è quello della crittazione attraverso chiave pubblica, ovvero un meccanismo di crittazione a chiave **asimmetrica**. Tali algoritmi si basano su un'accoppiata di chiavi:

una **chiave privata** segreta ed una **chiave pubblica** disponibile per tutti i richiedenti su rete. Esse sono generate contemporaneamente e attraverso un particolare algoritmo consentono di criptare e rispettivamente decriptare dei contenuti digitali. Ciò che si cripta con una chiave si decripta con l'altra e viceversa. La combinazione di queste possibilità consente di raggiungere obbiettivi di autenticità (essere certi di chi ci sta fornendo certe informazioni), confidenzialità (essere certi che solo ci è autorizzato acceda a certe informazioni) e integrità (essere certi che le informazioni che si trasferiscono non vengano modificate).

Una chiave pubblica è contenuta in un **certificato digitale** che inoltre associa questa chiave alle informazioni sul proprietario della chiave e sulla autorità che ha emesso il certificato. Se l'utente ha confidenza dell'autorità e può verificare la sua firma presente nel certificato, allora può confidare sul fatto che la chiave pubblica è del soggetto indicato nel certificato.

Il meccanismo per stabilire una connessione HTTPS combina una crittazione asimmetrica (per trasferire la chiave simmetrica) con una crittazione simmetrica (per proteggere il contenuto della trasmissione) ed è schematizzato qui sotto:

1- Il browser richiede al server una connessione sicura
2- Il server restituisce al client un certificato SSL
3- Il browser produce una **chiave di sessione** (meccanismo di crittazione a chiave simmetrica) da usare per criptare il traffico e la invia al server criptata con la sua chiave pubblica SSL.
4- Il server decritta la chiave di sessione con la sua chiave privata SSL (è l'unico che può farlo) e comunica al browser che le future trasmissioni saranno criptate con la chiave di sessione.
5- Server e browser iniziano a scambiarsi comunicazioni criptate.

Questa combinazione elimina gli svantaggi della crittazione simmetrica (la necessità di trasmettere la chiave di crittazione/decrittazione) e quelli della crittazione asimmetrica (gli algoritmi sono in generale molto più lenti) sfruttando i relativi vantaggi.

Per poter stabilire una connessione HTTPS è necessario quindi un certificato SSL lato server. Questo certificato può essere di diversi tipi e essenzialmente le principali tipologie sono:

- **self signed** (rilasciato dall'utente stesso e non da una CA)
- **domain validation** (rilasciato da una CA, ma verificando solo che il richiedente sia il proprietario del sito per cui è richiesto il certificato)
- **fully authenticated** (rilasciato da una CA, ma con una procedura più complessa che valida più aspetti)

In questo momento è stato utilizzato il primo tipo di certificato, ma nel momento in cui si andrà in produzione è necessario al meno un domain validation.

Per la generazione del certificato si è utilizzato un'utilità Java chiamata **keytool**: questa utilità permette di generare un file di tipo Java Keystore che serve per proteggere le chiavi private attraverso un password. Un Keystore è quindi un DB (un file in questo caso) che contiene la chiave pubblica, il certificato ad essa associato (con relative informazione della CA) e la chiave privata. Il programma keytool si trova nella cartella bin della JRE.

E' stata utilizzata la macchina di test **X.X.X.X** dove è stato installato un Apache Tomcat 6.0.14 e una JRE 1.6.0.03.

Per generare il Keystore si lancia l'utilità con la seguente sintassi:

```
keytool -genkey -alias <alias> –dname <distinguished name> -keyalg <alg> -
keystore <file name>
```

le opzioni utilizzate hanno questo significato:

-**genkey**: richiede di generare una coppia di chiavi pubblica/privata. La chiave pubblica è mantenuta in un certificato X.509v.1
-**alias**: è il nome del record nel keystore in cui sono memorizzate certificato e chiavi.
-**keyalg**: è l'algoritmo utilizzato per generare la coppia chiave pubblica/privata
-**keystore**: il nome del file che implementa il DB
-**dname**: è il distinguished name e rappresenta nel certificato l'identità del richiedente

Al momento della generazione del keystore viene richiesta una password di protezione del file ed una specifica della entry generata.

Nello specifico caso il comando utilizzato è stato:

```
keytool -genkey -alias tomcat -keyalg RSA -dname "CN=Stefano Pezzi, OU=progetti,
O=sinergis, L=bologna, ST=bo, C=it" -keystore c:/.keystore
```

Il file c:\.keystore generato va poi spostato in una cartella raggiungibile da Tomcat (e possibilmene protetta); nel nostro caso nella cartella C:\Tomcat6014\conf.

A questo punto occorre configurare Tomcat per attivare il connettore HTTPS.

Nel file $CATALINA_HOME/conf/server.xml e scommentare la seguente sezione:

```
<!--
    <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
               maxThreads="150" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS" />
-->
```

e aggiungere le informazioni circa il file keystore, la entry da ricercare e la password per accedervi:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
               maxThreads="150" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS"
               keystoreFile="C:\Tomcat6014\conf\.keystore"
               keystorePass="stefanopezzi"
              keyalias="tomcat">
```

```
</Connector>
```

Per ultimo occorre disattivare il connettore HTTP commentando nello stesso file la sezione:

```
    <Connector port="8081" protocol="HTTP/1.1"
       connectionTimeout="20000"
       redirectPort="8443" />
```

L'url del Geoserver di test è:

https://X.X.X.X:8443/geoserver/web/

4.2.1. Verifica compatibilità client

Riguarda la possibilità di utilizzare i diversi client GIS con i servizi WMS/WFS esposti su HTTPS e richiedenti l'identificazione dell'utente mediante HTTP Basic Authentication.
I test sono stati effettuati con i servizi protetti esposti dal progetto governativo australiano SLIP (Shared Land Information Platform) che espone WMS e WFS su protocollo HTTPS e protetti da utente e password (occorre semplicemente registrarsi per ottenerli). I servizi sono disponibili all'indirizzo:

https://www2.landgate.wa.gov.au/slip/portal/services/access-slip.html

Client GIS	Versione	SSL	HTTP Basic Authentication
uDig	1.1	SI	SI
Gaia	3.4	SI	SI
gvSIG	1.9	?	NO
QGIS (enceladus)	1.4.0	NO	SI
ArcMap	9.3	SI	SI
ArcExplorer Java	9.3.1	SI	SI
GoogleEarth	5.1.3533	SI	SI
OpenJUMP	1.3.0	NO	NO

4.2.2. Problemi correlati

Attualmente il traffico HTTP dell'indirizzo pubblico del server webgis.regione.sardegna.it (X.X.X.X) sulla porta 443 (HTTPS) è ridiretto sul server Citrix del progetto SIT2COM. Se si volesse attivare in parallelo ai servizi WMS/WFS in chiaro anche i servizi su protocollo sicuro HTTPS con uguale indirizzo a parte il protocollo occorrerebbe un nuovo indirizzo pubblico da assegnare o al server Citrix o a questi servizi, ad esempio:

https://webgis2.regione.sardegna.it/geoserver/ows?service=WMS

4.3. Collegamento Tomcat a LDAP

E' possibile configurare Tomcat affinché recuperi le credenziali di autenticazione da un server LDAP piuttosto che dal file di configurazione server.xml.

Al momento l'unico utente che viene utilizzato in Tomcat è l'utente amministratore "manager" che ha diritto di accedere appunto alla console di amministrazione che consente ad esempio di eseguire deploy e undeploy delle web application.

Questo utente, seppur unico, è replicato nelle 12 istanze di Tomcat presenti al momento nella IDT: trasferendo su LDAP le credenziali si elimina questa notevole duplicazione; contemporaneamente si dovrà eliminare l'utente applicativo attuale "manager" e sostituirlo con uno o più utenti personali.

Condizione necessaria è che il server LDAP sia a conoscenza di uno schema standard per la modellazione di organizzazioni di persone tipo "inetOrg" o "XXX". I ruoli possono essere modellati nell'LDAP o come "group" che contengono gli "user" oppure come attributi degli user. La configurazione di Tomcat dipende ovviamente da quale soluzione si è scelto.
Infatti, nel file di configurazione server.xml, con una sintassi che vedremo qui di seguito, si specifica la query che Tomcat dovrà eseguire verso il server LDAP. Si specificano infatti i parametri che dovranno essere sostituiti dinamicamente con le stringhe inserite dall'utente che si autentica.

```
<Realm   className="org.apache.catalina.realm.JNDIRealm" debug="99"
              connectionURL="ldap://localhost:389"
              userPattern="uid={0},ou=people,dc=mycompany,dc=com"
              roleBase="ou=groups,dc=mycompany,dc=com"
              roleName="cn"
              roleSearch="(uniqueMember={0})"
/>
```

La sezione di file XML mostrata va inserita nel file server.xml presente nella cartella %CATALINA_HOME%/conf di Tomcat. Il significato degli attributi dell'elemento Realm è il seguente:

className = nome della classe Java da utilizzare per la gestione del dominioTomcat. Deve valere ="org.apache.catalina.realm.JNDIRealm".

connection URL = url del server LDAP. Occorre utilizzare lo schema ldap:.

userPattern = il Distinguished Name dello user nell'LDAP che Tomcat utilizzerà nell'operazione di binding per l'autenticazione dell'utente. Contiene pattern di sostituzione per indicare il parametro che andrà sostituito con il valore dello username indicato dall'utente che si connette.

roleBase = il Relative Name dove si collocano i ruoli nell'albero LDAP

roleName = nome dell'attributo del ruolo sul quale effettuare il binding

roleSearch = la clausola di ricerca per selezionare. Può contenere i pattern di sostituzione.

I pattern di sostituzione utilizzati hanno significato diverso a seconda dell'attributo in cui sono utilizzati e sono:

In `userPattern`
`{0} = user name`

In `roleSearch`
`{0} = Distinguished name`
`{1} = user name`

Un vincolo di questa configurazione è che il contenuto del roleName che abilita il manager di Tomcat sia proprio la stringa "manager". Questa obbligo può essere facilmente superato utilizzando ad esempio un attributo differente rispetto al cn (Common Name). In questo modo si può continuare ad utilizzare la naming convention voluta per i nomi dei ruoli; ad esempio: se utilizziamo il nome

cn = role_idt_tomcat_manager

Possiamo utilizzare l'attributo

businessCategory = manager

ed impostare in server.xml

`roleName =` businessCategory

ATTENZIONE: Tomcat non si avvierà se il server LDAP non è attivo.

4.4. Collegamento Apache a LDAP

Nella IDT sono presenti 3 installazioni dei web server Apache (ciascuna replicata sui nodi ridondanti):

- web server
- application server
- map server

Mentre è chiaro il compito degli Apache sui due web server (sitrs4004, sitrs4005) che espongono sulla internet tutti i servizi della IDT passando attraverso un nodo dove è installato il Network Load Balancing (NLB) Microsoft, il compito degli Apache sul map server è più specifico: essi servono le immagini create su disco da ArcIMS.

Gli Apache sugli application server sono invece in questo momento non utilizzati.

Gli Apache esterni rigirano le chiamate ai contenitori di applicazioni (Tomcat o JBOSS) degli application server (meccanismo di proxy) attraverso il protocollo AJP oppure verso gli Apache installati sui map server attraverso il protocollo HTTP.

Per gestire la funzionalità di proxy sono caricati due moduli:

- mod_proxy
- mod_proxy_ajp

Oltre a questi due moduli viene caricato il

- mod_proxy_balancer

per gestire un bilanciamento del carico verso gli application server.

Il mod_proxy_balancer offre un'interfaccia di amministrazione**Errore. Riferimento a collegamento ipertestuale non valido.**. Attualmente questa applicazione non è protetta da meccanismi di controllo degli accessi, ma sarebbe opportuno attivarli attraverso le funzionalità relative che offre Apache.

Per attivare meccanismi di protezione su Apache è necessario caricare alcuni moduli; nello specifico caso, volendo utilizzare una directory utenti LDAP come sistema di autenticazione, è necessario caricare i moduli:

```
LoadModule ldap_module modules/mod_ldap.so
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
```

A questo punto, nel file di configurazione di Apache httpd.conf, è possibile inserire negli elementi <Directory> o <Location> che si desiderano proteggere delle direttive che obbligano Apache a interrogare la LDAP prima di consentire l'accesso.
E' possibile configurare l'accesso a LDAP in maniera differente in modo da abilitare policy basate sull'utente o sul ruolo.
Un esempio banale è il seguente:

```
<Directory /esempio>
  AuthType Basic
  AuthName "Area protetta"
  AuthBasicProvider ldap
  AuthzLDAPAuthoritative   On
  AuthLDAPURL ldap://<server ldap>:<porta>/<dn>?<attributo della ricerca>"
  Require valid-user
</Directory>
```

In questo caso si indica ad Apache di effettuare una operazione di *search/bind* sul server ldap `<ldap server>` con il protocollo LDAP sulla porta `<porta>` a partire dalla posizione `<dn>` impostando la ricerca sull'attributo `<attributo della ricerca>`. La policy di autorizzazione è quella esplicitata nell'ultima direttiva `Require valid-user` che indica che è richiesta la semplice indicazione di un utente valido, ovvero presente nella directory LDAP.

Vediamo qui sotto il significato di alcune direttive da utilizzare:

AuthType: seleziona il protocollo per il trasporto delle credenziali di autenticazioni. Si può scegliere tra basic o digest, che sono le modalità standard supportate da HTTP.

AuthName: Nome del dominio di autenticazione (compare nella finestra che il browser mostra all'utente).

AuthBasicProvider: Tipo di autenticazione; indicando "ldap" si specific ache si intende accedere ad un server LDAP.

AuthLDAPUrl: La URL del server LDAP. In questa URL sono specificati diversi parametri (secondo lo standard RFC2255). Si specificano sia il server ma anche i parametri di ricerca, in questo modo:

```
ldap://host:port/basedn?attribute?scope?filter
```

dove

- ldap: esprime il protocollo; può essere anche ldaps, per ill dap su SSL
- host: nome o IP del server LDAP
- port: porta alla quale risponde il server
- basedn: il ramo dell'albero LDAP da cui devono incominciare le ricerche
- attribute: l'attributo che contiene il nome dell'utente
- scope: esprime quanto in profondità si desidera effettuare la ricerca; il valore può essere "one" (un solo livello sotto il ramo base) oppure "sub" (tutti i livelli esistenti)
- filter: filtro aggiuntivo da aggiungere alla ricerca

AuthzLDAPAuthoritative: se impostato a "on" impedisce l'intervento di altri moduli di autenticazione se fallisce quella LDAP.

Require <type>: Specifica chi è autorizzato ad accedere alla cartella protetta. E' possibile specificare il nome di uno o più utenti o gruppi oppure un file dove sono inserite queste informazioni.

Occorre sottolineare anche che al fine di ottimizzare le prestazioni Apache effettua il caching delle operazioni di search/bind per default. In fase di debugging o test (mentre cioè si modificano spesso autorizzazioni e contenuto della LDAP) è quindi consigliabile disabilitare tale opzione con la direttiva:

```
LDAPCacheEntries 0
```

Il caso che ci interessa è quello dove si abilita l'accesso ad un utente perché appartiene ad un certo gruppo ovvero possiede un certo ruolo.

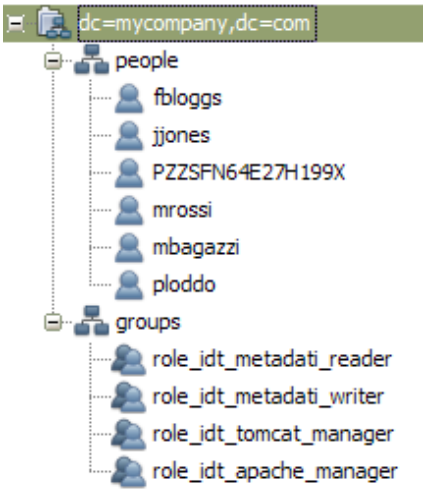


Figura 3 - Directory utenti di esempio

Supponiamo allora di avere una situazione illustrata nella Figura 3 all'interno della directory LDAP. In questa situazione il ruolo che abilita alla gestione del load balancing di Apache è il ruolo "role_idt_apache_manager" al quale sono associati alcuni utenti mediante l'uso dell'attributo "uniqueMember".

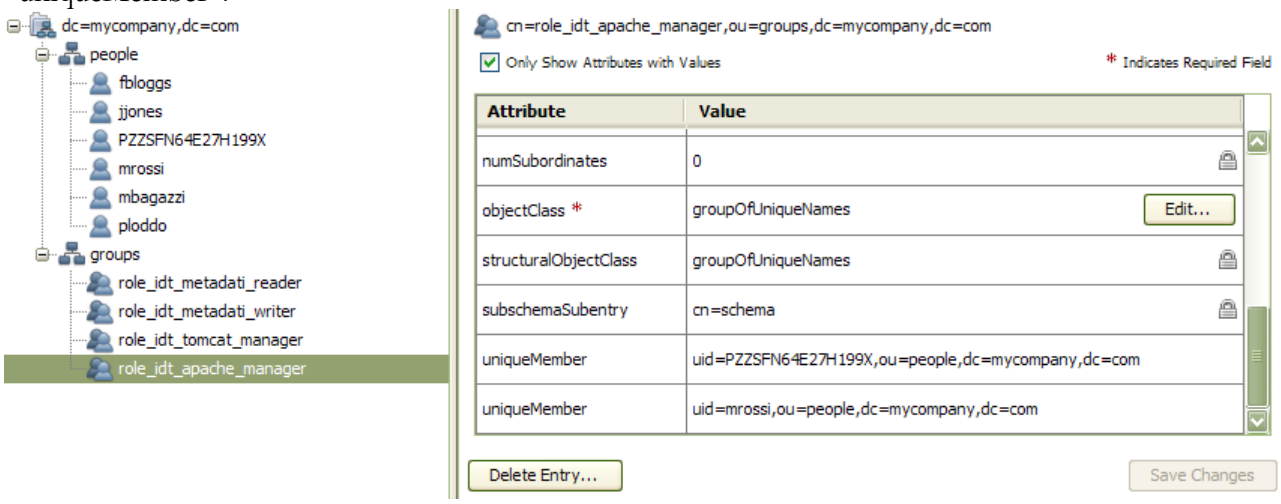


Figura 4 - Utente appartenente ad un ruolo

La configurazione di Apache dovrà quindi essere:

```
<Directory d:/esempio>
    AuthType Basic
    AuthName "Area Protetta"
    AuthBasicProvider ldap
    AuthzLDAPAuthoritative   on
```

```
    AuthLDAPURL ldap://pezzicore:389/ou=people,dc=mycompany,dc=com?uid?sub?
    AuthLDAPGroupAttribute uniqueMember
    AuthLDAPGroupAttributeIsDN on
    Require ldap-group cn=role_idt_apache_manager,ou=groups,dc=mycompany,dc=com
</Directory>
```

In questo caso si sono aggiunte le direttive

AuthLDAPGroupAttribute: attributo dell'elemento "group" che contiene i membri.

AuthLDAPGroupAttributeIsDN: specifica (se "on") che in tale attributo sono memorizzati i Distinctive Name (dn) anziché i Common Name (cn) degli utenti.

4.5. Utenti e ruoli Oracle

4.5.1. Schemi Oracle

Separazione degli schemi condivisi secondo la suddivisione logica del DB Unico: IDT, MD e FC. Gli utenti corrispondenti a tali schemi saranno utilizzati per creare gli oggetti e poi non saranno più utilizzati (questo vale anche per lo schema IDT dove la creazione degli oggetti sarà effettuata però dagli utenti applicativi corrispondenti a vari gruppi di processi di ETL).
Lo schema da creare è quello FC i cui oggetti saranno da trasferire dall'attuale schema IDT. L'applicazione andrà riconfigurata per accedere a tale schema e dovrà essere prodotto un nuovo rilascio con documentazione aggiornata.

4.5.2. Ruoli

Per una gestione più semplice e corretta delle autorizzazioni su Oracle è necessario passare sempre attraverso i ruoli; anche se ci fosse una corrispondenza 1:1 con ruoli di sistema o ci fosse un solo utente da associare il ruolo è buona regola creare sempre ruoli specifici.

Per la nomenclatura dei ruoli da utilizzare occorre adoperare uno standard come ad esempio "ROLE_IDT_XXX" in modo da poter individuare immediatamente i ruoli creati.

4.5.3. Utenti personali

Anche in assenza di integrazione con la directory utenti di rete, è auspicabile sostituire tutti gli utenti impersonali (vedi quelli dei sistemisti) con relativi utenti personali. Oltre a questo è importante non attribuire direttamente agli utenti i privilegi sui diversi oggetti di DB o i privilegi di sistema, ma passare sempre attraverso ruoli. Gli utenti impersonali utilizzati al momento sono:

- SYS
- SYSTEM

Si tratta quindi di creare i seguenti utenti personali:

- XXXXXXXX
- XXXXXXXX
- XXXXXXXX

Ed attribuire loro il ruolo di DBA, o meglio di ROLE_IDT_DBA .

E' necessario inoltre definire gli utenti che si collegheranno direttamente al DB per visualizzare i dati vettoriali della IDT attraverso client GIS, sia quelli per i dati liberi che quello per i dati protetti.

4.5.4. Utenti applicativi

Le applicazioni three-tier saranno configurate con utenti applicativi Oracle dotati di permessi limitati e congruenti con gli obbiettivi delle applicazioni stesse. Verranno quindi creati nuovi utenti applicativi in alcuni casi ed in altri dovranno essere cambiati anche gli schemi (utenti che posseggono gli oggetti di DB).
Per uniformità di gestione, l'assegnazione dei privilegi è meglio che passi attraverso un ruolo (ROLE) anche se esisterà un unico utente associato a tale ruolo.

La modalità di autenticazione degli utenti applicativi può essere mantenuta interna (database).

Un esempio è il Gestore Feature Catalogue che ha le proprie tabelle all'interno dello schema IDT e a cui accede con il medesimo utente. In questo caso:

- verrà creato un nuovo schema per ospitare le tabelle (es.: FC)
- sarà assegnato un utente applicativo (es.: 0002-FC-WRITE) senza il ruolo di RESOURCE, ma con i necessari privilegi di SELECT, INSERT, DELETE e UPDATE sugli oggetti di tale schema ed il ruolo di CONNECT.
- Tali privilegi verranno assegnati non direttamente all'utente, ma attraverso un ruolo ROLE_IDT_FC_WRITE.

In sintesi gli utenti ed i ruoli da creare in Oracle sono indicati dalla tabella seguente:

role
ROLE_IDT_DBA
ROLE_IDT_DTS_FREE_READER
ROLE_IDT_DTS_PROT_READER
ROLE_IDT_DTS01_READER
ROLE_IDT_DTS02_READER
ROLE_IDT_DTS03_READER
ROLE_IDT_DTS04_READER
ROLE_IDT_DTS05_READER

ROLE_IDT_DTS06_READER
ROLE_IDT_DTS07_READER
ROLE_IDT_DTS08_READER
ROLE_IDT_DTS09_READER
ROLE_IDT_DTS10_READER
ROLE_IDT_DTS11_READER
ROLE_IDT_DTS12_READER
ROLE_IDT_DTS13_READER
ROLE_IDT_DTS14_READER
ROLE_IDT_APP_MD_READER
ROLE_IDT_APP_MD_WRITER
ROLE_IDT_APP_FC_READER
ROLE_IDT_APP_FC_WRITER
ROLE_IDT_DTS01_RESOURCE
ROLE_IDT_DTS02_RESOURCE
ROLE_IDT_DTS03_RESOURCE
ROLE_IDT_DTS04_RESOURCE
ROLE_IDT_DTS05_RESOURCE
ROLE_IDT_DTS06_RESOURCE
ROLE_IDT_DTS07_RESOURCE
ROLE_IDT_DTS08_RESOURCE
ROLE_IDT_DTS09_RESOURCE
ROLE_IDT_DTS10_RESOURCE
ROLE_IDT_DTS11_RESOURCE
ROLE_IDT_DTS12_RESOURCE
ROLE_IDT_DTS13_RESOURCE
ROLE_IDT_DTS14_RESOURCE
ROLE_IDT_FC_RESOURCE
ROLE_IDT_IDT_RESOURCE
ROLE_IDT_MD_RESOURCE

Tabella 30 - Ruoli Oracle da definire

utenti	role
XXXXXXXX	ROLE_IDT_DBA
XXXXXXXX	ROLE_IDT_DBA
XXXXXXXX	ROLE_IDT_DBA
<utenti personali lettori catasto>	ROLE_IDT_DTS01_READER
<utenti personali lettori dati liberi>	ROLE_IDT_DTS_FREE_READER
0002-FC	ROLE_IDT_APP_FC_WRITER
0003-MD-R	ROLE_IDT_APP_MD_READER
0003-MD-W	ROLE_IDT_APP_MD_WRITER
0004-GEOS1	ROLE_IDT_DTS_FREE_READER
0005-GEOS2	ROLE_IDT_DTS_PROT_READER
0010-AIMS	ROLE_IDT_DTS_FREE_READER
0025-SCAR	ROLE_IDT_DTS_FREE_READER
1001-ETL	ROLE_IDT_DTS01_RESOURCE
…	
1014-ETL	ROLE_IDT_DTS1_4RESOURCE
FC	ROLE_IDT_FC_RESOURCE
IDT	ROLE_IDT_IDT_RESOURCE
MD	ROLE_IDT_MD_RESOURCE

Tabella 31 - Utenti Oracle da definire

4.5.5. Tablespace

Per poter raggruppare le tabelle dello schema IDT, che costituiscono la componente vettoriale del DBUnico, in gruppi (dataset) al fine di facilitare la gestione delle autorizzazioni è possibile ipotizzare l'utilizzo del concetto di TABLESPACE. In altre parole, tabelle appartenenti al medesimo dataset possono venir create nello stesso tablespace oracle in modo da avere anche sul DB questo raggruppamento (se necessario, una tabella può venire spostata da un tablespace ad un altro con facilità).

4.5.6. Procedure a supporto della gestione autorizzazione su Oracle

Per facilitare la gestione delle autorizzazioni è conveniente sviluppare Stored Procedure che permettano di eseguire operazioni come assegnazione di un ruolo a tutte le tabelle di uno schema o di un dataset (tablespace).

4.6. Applicazioni

Interventi di sola configurazione (no sviluppo) sulle applicazioni esistenti sia web che desktop.

4.6.1. Utenti personali

Occorre sostituire gli utenti impersonali utilizzati al momento in applicazioni 3 tier o desktop (Es. "metadati", "fcuser1"…) con gli opportuni utenti personali (anche se la sincronizzazione delle password non è negli obbiettivi immediati e quindi il disallineamento delle credenziali inevitabile).

4.6.2. Attivazione utenti applicativi

Dovranno essere riconfigurati i servizi relativi lanciati al momento attraverso utenti di sistema locali

4.6.3. Client GIS

Gli utenti da utilizzare per la connessione al DB attraverso i client GIS desktop sono gli utenti personali definiti all'interno del DB stesso. Occorre fornire agli utilizzatori dei client le istruzioni per il collegamento e l'utilizzo dei dati.

4.6.4. Disattivazione applicazioni desuete

Occorre semplificare il sistema mediante la disattivazione di quelle applicazioni e/o servizi che con il tempo sono state rese desuete e sostituite da altre. In particolare i servizi ArcIMS per i dati vettoriali.

4.7. Utenti e gruppi di dominio Windows

Gli interventi suggeriti riguardanti gli utenti di rete dei domini Active Directory SITRS o UFFICIOPIANO sono:

- Eliminazione di tutti gli utenti locali dei server in dominio[28].
- Eliminazione di tutti gli utenti impersonali utilizzati da persone fisiche.
- Creazione di utenti applicativi di dominio per l'esecuzione dei servizi[29].
- Omogeneizzazione dei nomi degli utenti del dominio SITRS (in alternativa abbandono del dominio SITRS e utilizzo di un unico dominio UFFICIOPIANO, ma questa soluzione è improbabile).
- Eliminazione delle utenze duplicate nei due domini.
- Strutturazione degli utenti in gruppi ed Unità Organizzative.
- Privilegi e permessi su risorse sono da garantire esclusivamente a gruppi e non ad utenti singoli.

4.8. Storage condiviso

E' auspicabile che tutte le risorse disco condivise siano mantenute sull'unico dispositivo e che non si utilizzino cartelle locali ai server. Sule risorse dei server non devono accedere utenti che non siano amministratori degli stessi.

4.8.1. Protezione risorse di rete

Trasferimento delle cartelle condivise sui vari server sullo storage apposito e revisione delle policy di accesso alle risorse di storage condivise.

4.8.2. Ristrutturazione della cartella condivisa per dati raster

I dati raster al momento sono contenuti nella cartella "dati" (`urn:sitr:res:dir:0010-dati`). Per facilitare la gestione delle autorizzazioni si possono utilizzare sottocartelle per implementare il concetto di dataset composto da file in modo da attribuire i privilegi alle sole cartelle e non ai singoli file.
Si tratta quindi di creare la sottocartella "dati/fotoAeree" e di spostarvi i raster, riconfigurando di conseguenza le applicazioni ed i servizi che vi accedono.

[28] Da notare che i DB server (per via del Sistema Operativo) e i Web Server (che risiedono in DMZ) non appartengono al dominio di rete.
[29] In parte tali utenti sono già stati definiti.

5. Pianificazione attività

Di seguito la pianificazione e la stima delle attività descritte nel capitolo precedente, con l'eccezione delle attività riguardanti l'autenticazione esterna di Oracle e con le seguenti precisazioni riguardo le prime quattro:

1. Geoserver su HTTPS: installazione di 3 istanze di Geoserver (possibilmente v.2.x se nel frattempo verrà rilasciata la 2.0.2). Implica l'installazione e configurazione di 3 Tomcat in HTTPS sui tre map server dell'infrastruttura ed il trasferimento della catalogazione dei dati catastali dagli attuali Geoserver. L'esposizione del servizio in HTTPS potrà essere realizzata alternativamente all'attivazione di SSL sul back-end, anche attraverso una diversa configurazione di Apache (che fa da proxy per gli application server): la valutazione della soluzione più adatta verrà definita in fase di implementazione.
2. Middleware:
    a. Collegamento Apache ad LDAP e relativa configurazione firewall per DMZ.
    b. Collegamento Tomcat ad LDAP (tutti i Tomcat degli application e map server, compresi i nuovi in HTTPS).
3. Oracle: utenti e ruoli per le applicazioni Gestore Feature Catalogue, Gestore Metadati e Catalogo Metadati. Creazione dei table space per le FT (291) esistenti al momento ed i gruppi individuati dal censimento (14). Revisione dei corrispondenti ETL. Procedura per l'attribuzione dei permessi alle tabelle di un table space.
4. Applicazioni: le applicazioni interessate dalla riconfigurazione per gestire i nuovi utenti sono Gestore Feature Catalogue, Gestore Metadati e Catalogo Metadati. Queste andranno quindi riconfigurate e saranno oggetto di un nuovo rilascio (le DDL e la documentazione cambiano).

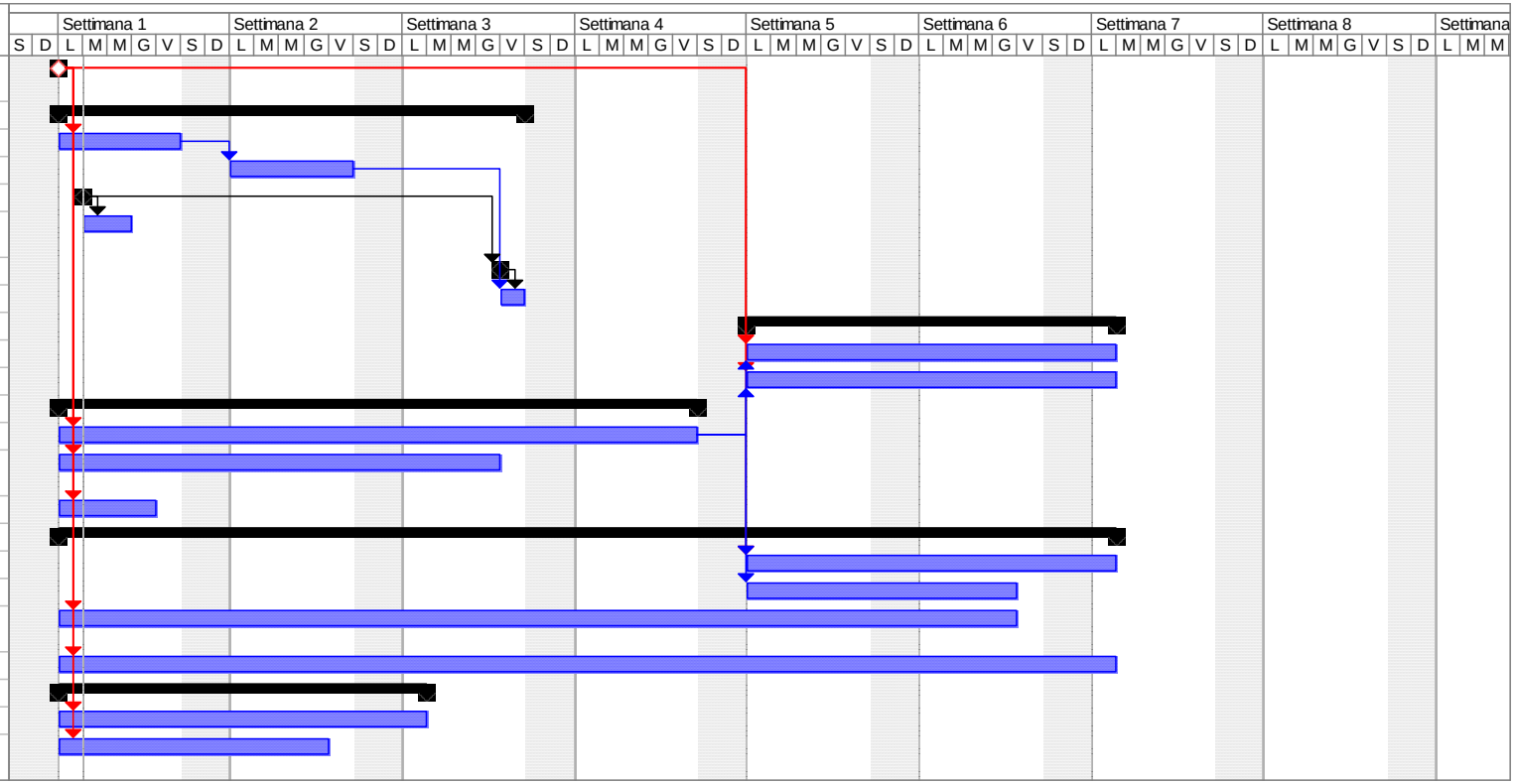
Attività	**AE**	**ABD**	**Presidio**
Geoserver HTTPS (par. 4.2)	2	3	8
Middleware (par 4.3, par. 4.4)		4	10
Oracle (par. 4.5)		2	7
Applicazioni (par. 4.6)	6	4	2
Utenti e gruppi Windows (par. 4.7)		1	10
Storage condiviso (par. 4.8)		1	3
TOTALE	**8**	**15**	**40**

NB.: per la realizzazione delle attività è necessario avere a disposizione l'ambiente di test ristrutturato così pure per definire i permessi sullo storage condiviso è necessario sia effettuata la migrazione del servizio Samba.

Tutte le operazioni riguardanti applicazioni in produzione, anche se interessanti solo la configurazione, saranno effettuate prima in ambiente di test e poi ripetute in produzione.

Nella pianificazione quindi è stata introdotta un'attività esterna (ristrutturazione Server Farm e predisposizione ambiente di test) da cui dipendono tutte le atttività di riordino.

ID	Nome attività
1	Ristrutturazione Server Farme predisposizione ambiente di test
2	**Geoserver su HTTPS**
3	Installazione Geoserver su HTTPS
4	Configurazione dati catastali
5	Richiesta nuovo IP pubblico
6	Pubblicazione notizia trasferimento dati protetti
7	Attribuzione nuovo IP
8	Attivazione nuovo url
9	**Middleware**
10	Collegamento Apache a LDAP
11	Collegamento Tomcat a LDAP
12	**Oracle**
13	Utenti e ruoli in Oracle
14	Sviluppo procedure a supporto autorizzazione Oracle
15	Tablespace
16	**Applicazioni**
17	Utenti personali e applicazioni
18	ClientGIS
19	Disattivazione applicazioni desuete
20	Utenti e gruppi Windows
21	**Storage condiviso**
22	Protezione risorse di rete
23	Ristrutturazione della cartella condivisa per dati raster



6. Considerazioni finali

I dati raccolti nel censimento sono numerosi e molto articolati come si può vedere dallo schema concettuale di Figura 1 e dalla sua implementazione nel DB Access allegato al presente documento.

La gestione di questo DB risulta piuttosto complessa e va ad aggravare i già non semplici processi di gestione della SDI. All'atto di introdurre un nuovo dato nella SDI, ad esempio, ai passi relativi alla catalogazione in Geoserver, in SDO, in SDE, nel Feature Catalogue e nel catalogo metadati si va ad aggiungere anche l'aggiornamento del DB Access, spesso replicando inutilmente le informazioni già inserite.

L'utilità di un catalogo del genere emerge solo quando questo catalogo diventa centralizzato (su un DB enterprise) e soprattutto quando esso costituisce l'unico catalogo in cui si inseriscono le informazioni, lasciando il compito di aggiornare gli altri cataloghi ad automatismi da implementare. In un tale scenario il "catalogo della SDI" non va a sostituire tutti gli altri cataloghi esistenti: Feature Catalogue e Catalogo Metadati ISO manterrebbero completamente la loro valenza in quanto le informazioni specifiche che loro contengono non verrebbero gestite nel catalogo SDI, che si limiterebbe invece a riportare solo gli identificativi degli elementi ivi catalogati. Essi sarebbero quindi semplicemente integrati nel catalogo SDI mantenendo la loro autonomia ed gli item contenuti sarebbero referenziati da quelli del catalogo SDI.

Stesso discorso vale per il package di A/A: se fosse implementato attraverso una soluzione di terze parti, le entità relative (users, roles, policy…) dovrebbero essere scorporate dal catalogo e si dovrebbe realizzare una integrazione con tale sistema. Per fare un esempio, supponiamo di utilizzare il prodotto IAM di Oracle (OIM); all'atto di definire una policy di autorizzazione all'interno di OIM, per proporre all'amministratore la scelta delle risorse da attribuire alla policy, OIM dovrebbe interrogare il catalogo per ottenere la lista di tutte le risorse possibili.

Nell'architettura SITR/SDI questo catalogo andrebbe a far evolvere quello che era il ruolo del Repertorio Metadati Applicativi previsto dal progetto iniziale, implementandone le funzionalità e correggendone i punti deboli (vedi, ad esempio, la presenza di una sistema di A/A integrato).

Per esemplificare l'utilizzo del Catalogo SDI, prendiamo in esame il processo di gestione "introduzione di un nuovo dato nella SDI" e vediamo come potrebbe essere semplificato e migliorato attraverso l'utilizzo del catalogo e del software che vi andrebbe sviluppato sopra. Supponiamo che

- i dati da introdurre costituiscano un dataset unico sia dal punto di vista della metadatazione (una sola scheda, quind) che dal punto di vista delle procedure di caricamento,
- tale il dataset sia composto da due tabelle Oracle,
- ciascuna delle tabelle rappresenta una Feature Type,
- ciascuna FT produca un solo layer (WMS)
- i layer vengano aggiunti ad una mappa esistente di libera consultazione (SardegnaMappe)

- le Feature Type vengano invece inserite in una lista di feature il cui accesso è limitato a utenti con certe caratteristiche (WFS protetto)

Il dataset in questione potrebbe essere costituito dalle Aziende Agricole (geometria poligonale rappresentante gli edifici destinati all'attività agricola), le relative Colture (geometria poligonale rappresentante gli appezzamenti derivanti dalla cartografia catastale) e dati alfanumerici, anagrafici per le aziende e qualitativi/quantitativi per i terreni.

Ecco quali potrebbero essere i passi del processo:

0. Consegna da parte del proprietario del dato di DB operazionale, informazioni sulla struttura del dato, metadati, specifiche di protezione. Il DB operazionale sia costituito, ad esempio, da un DB Access e da alcuni shape, i metadati dal modello Word predisposto dal SITR opportunamente riempito e le specifiche di protezione da indicazioni discorsive.

1. Predisposizione del DB Operazionale da cui prelevare il dato sulla cartella apposita (cartella nel dispositivo di storage condiviso su cui possono leggere solo i processi di ETL).

2. Analisi dei dati e individuazione delle Feature Type; modellazione degli schemi relativi (struttura degli attributi, tipologia, domini). Attività completamente non "automatizzabile", basata sulle informazioni consegnate, ulteriori e inevitabili delucidazioni e su analisi statistiche sui dati.

3. Catalogazione della Feature Type all'interno del Feature Catalogue → tale operazione, mediante un automatismo, ad esempio un Web Service, porta alla creazione nel Catalogo SDI dell'ID delle FT e del relativo loro riferimento nel catalogo FT).

4. Sviluppo dell'ETL di caricamento/trasformazione del dato (potrebbe essere in parte ricavato da una query nel FC, in particolare la DDL di creazione dei Geodata su Oracle se si tratta di dato vettoriale).

5. Sviluppo dell'ETL di estrazione e produzione del pacchetto di scarico.

6. → Catalogazione degli ETL nel Catalogo SDI (gli ETL sono così collegati alle FT)

7. Esecuzione degli ETL: vengono creati quindi i Geodata (in questo caso le tabelle spaziali Oracle e SDE all'interno del DBUnico) ed i pacchetti di scarico. L'esecuzione potrebbe essere lanciata anche da Catalogo SDI. → L'ETL registra anche i GeoData ed i pacchetti di scarico all'interno del Catalogo SDI collegandoli alle FT); questo modulo dell'ETL può essere un modulo comune riutilizzato da tutti gli ETL.

8. → Creazione del Dataset nel Catalogo SDI costituito dai due Geodata (l'operazione scatena una chiamata ad un Stored Procedure Oracle che crea il TableSpace corrispondente al gruppo e vi sposta le tabelle create).

9. Si passa ora su Catalogo MD e si crea la scheda per il Dataset (→ via WS l'operazione si crea l'ID del Metadato all'interno del Catalogo SDI e lo collega al dataset). → Nella scheda metadato si può mettere il riferimento alla FT (nome FT e ID catalogo), come previsto dallo standard ISO.

10. Si definiscono ora gli stili per produrre i layer: questo può essere fatto attraverso un editor di SLD (es.: uDIG) oppure con un editor XML.

11. → Si catalogano gli stili nel Catalogo SDI associandoli alle FT. Questa operazione può scatenare una validazione poiché nel Feature Catalogue sono contenute le informazioni necessarie a verificare se le regole sono corrette (nome dei campi, domini…).

12. → Con il Catalogo SDI si associano i layer ad una Mappa esistente esposta attraverso un servizio WMS e attraverso il navigatore Sardegna2D e/o SardegnaMappe. Si associano inoltre le FT ad una lista di FT esistente ed esposta attraverso un WFS protetto.
Queste operazioni scatenano la catalogazione nei Geoserver della IDT attraverso le API REST di amministrazione e l'aggiunta dei layer al file XML del servizio ArcIMS su cui si basa Sardegna2D (non consideriamo in questo scenario il repertorio). Anche il file XML di configurazione di SardegnaMappe può essere modificato automaticamente. Nella catalogazione dei Layer il sistema introduce automaticamente le informazioni di collegamento alla scheda metadato ed al pacchetto di scarico, informazioni che saranno disponibili nella GetCapabilities del WMS.

A questo punto i layer sono disponibili attraverso il WMS, una mappa Sardegna2D ed una SardegnaMappe. Le FT saranno invece disponibili sul WFS protetto del Geoserver esposto su HTTPS.
I metadati saranno ricercabili e consultabili sul catalogo dati e così nel FC si potranno trovare le informazioni sulla struttura del dato.

La scheda metadati conterrà il link al Feature Catalogue per interrogare le Feature Type.

Dal WMS e dai client che l'utilizzano si potrà accedere al metadato o al link per il download.

I dati saranno accessibili anche via client SDO o SDE internamente alla rete.