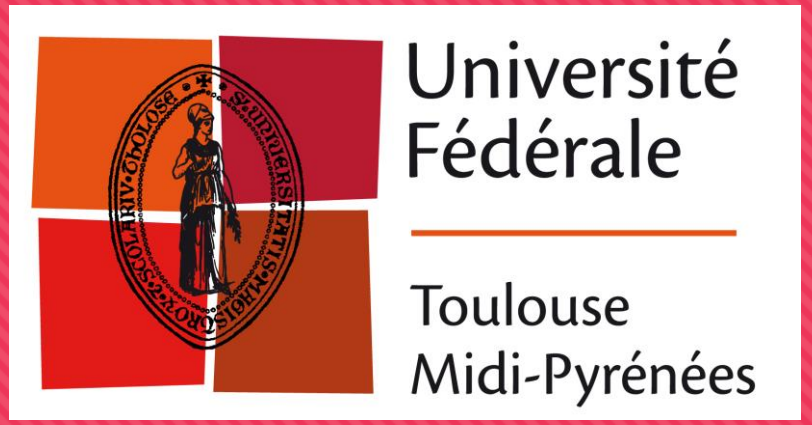


Architecture d'authentification unifiée pour la plateforme UNR

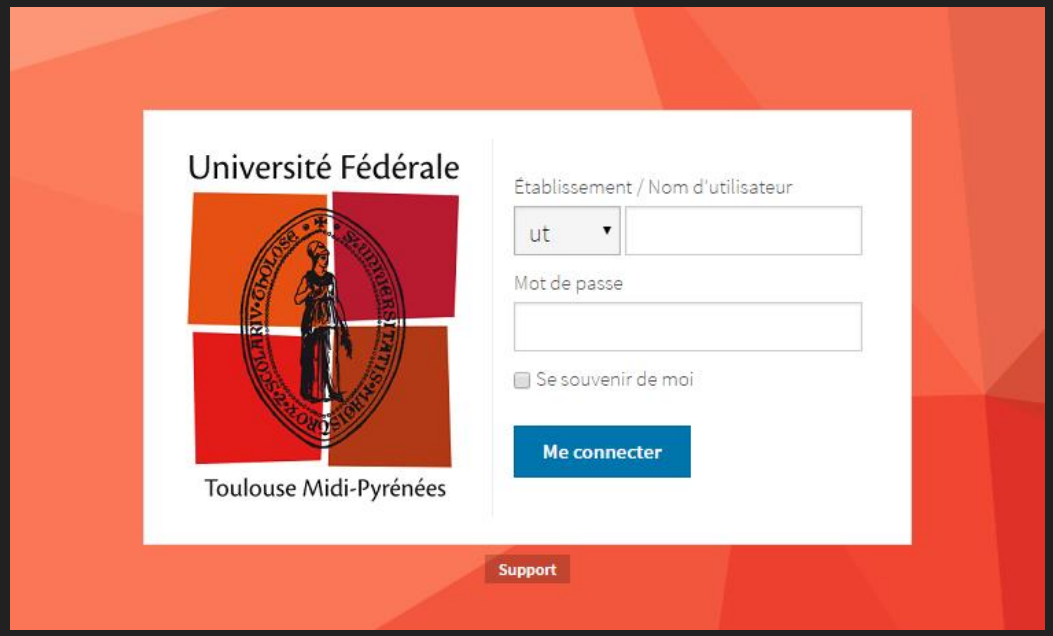
Louis Chanouha & Florent Lartet – Capitoul – 13 octobre 2016

Introduction

- UNR – depuis 2008
  - Un CAS Jasig, un annuaire LDAP central, des annuaires établissement
  - Modifié : gestion des contextes établissement
  - Un comportement: fusion des comptes
- Une évolution nécessaire
  - Sécurité & maintenance
  - Nouveaux usages
  - Fin de support matériel
- Nouvelle infrastructure
  - « il faut tout (re)faire »

Plan

- Introduction : une évolution nécessaire
- I – **Annuaire LDAP unifié, fédération d'identité**
- II – Du CAS Apereo au CAS Casino
- III – Évolutions du CAS
- IV – Architecture finale, haute disponibilité
- V – Vers la fédération d'identité Shibboleth
- Conclusion

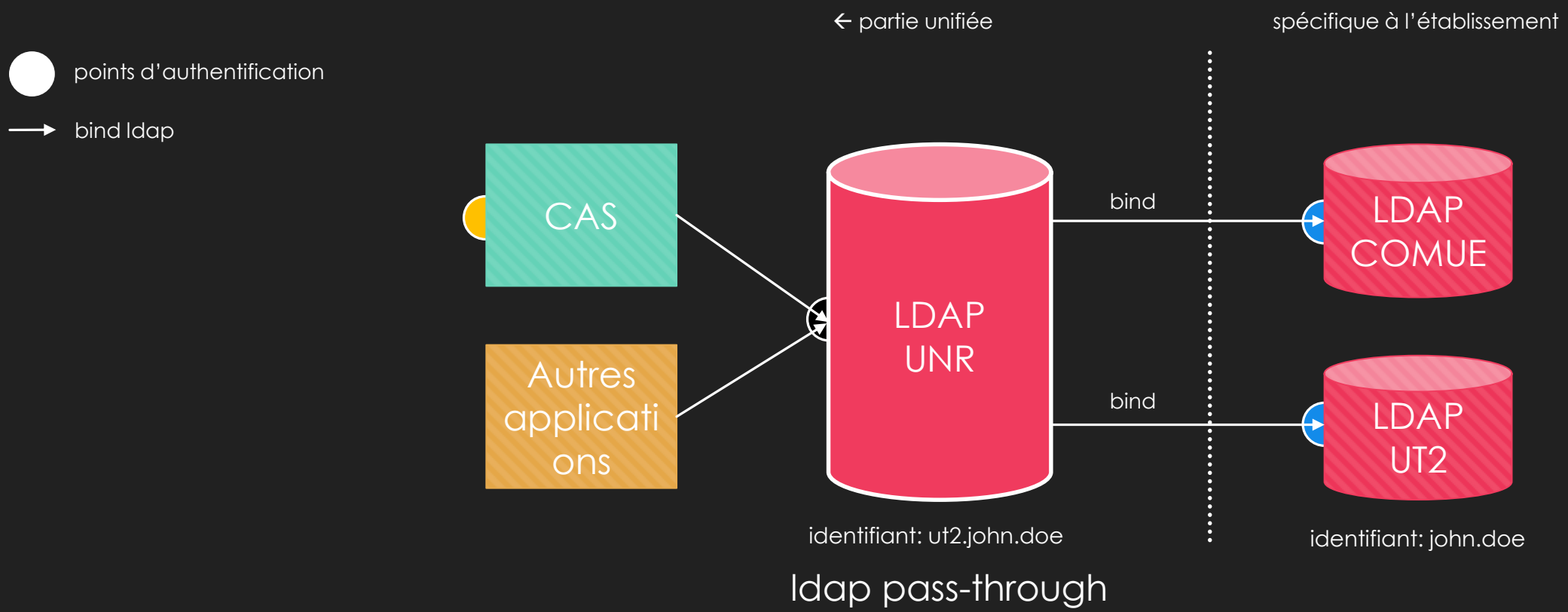


II – Annuaire et fédération d'identité (1)

- Socle LDAP pass-through
  - **Permet d'authentifier un utilisateur en ciblant un établissement sans information spécifique de la part de l'utilisateur**
  - Abstraction faite au niveau de l'annuaire UNR
    - Une branche LDAP par établissement
  - Construit à base de remontées LDIF
  - Autres usages que l'authentification (routage courriel, alias, support OTRS)

I - Annuaire et fédération d'identité (2)

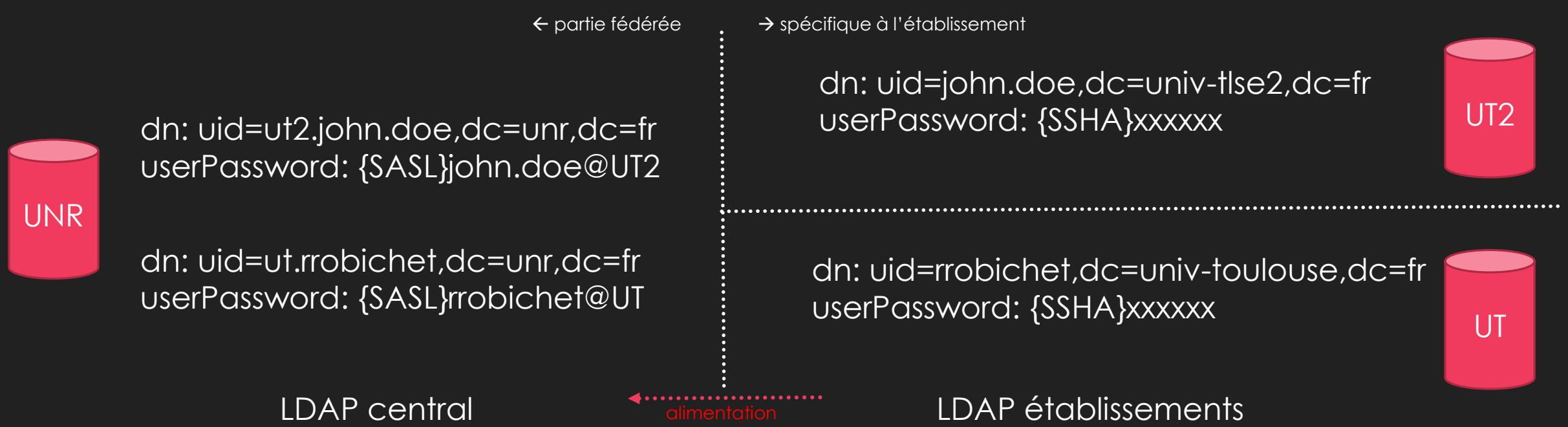
- Annuaire – architecture logique



ldap pass-through

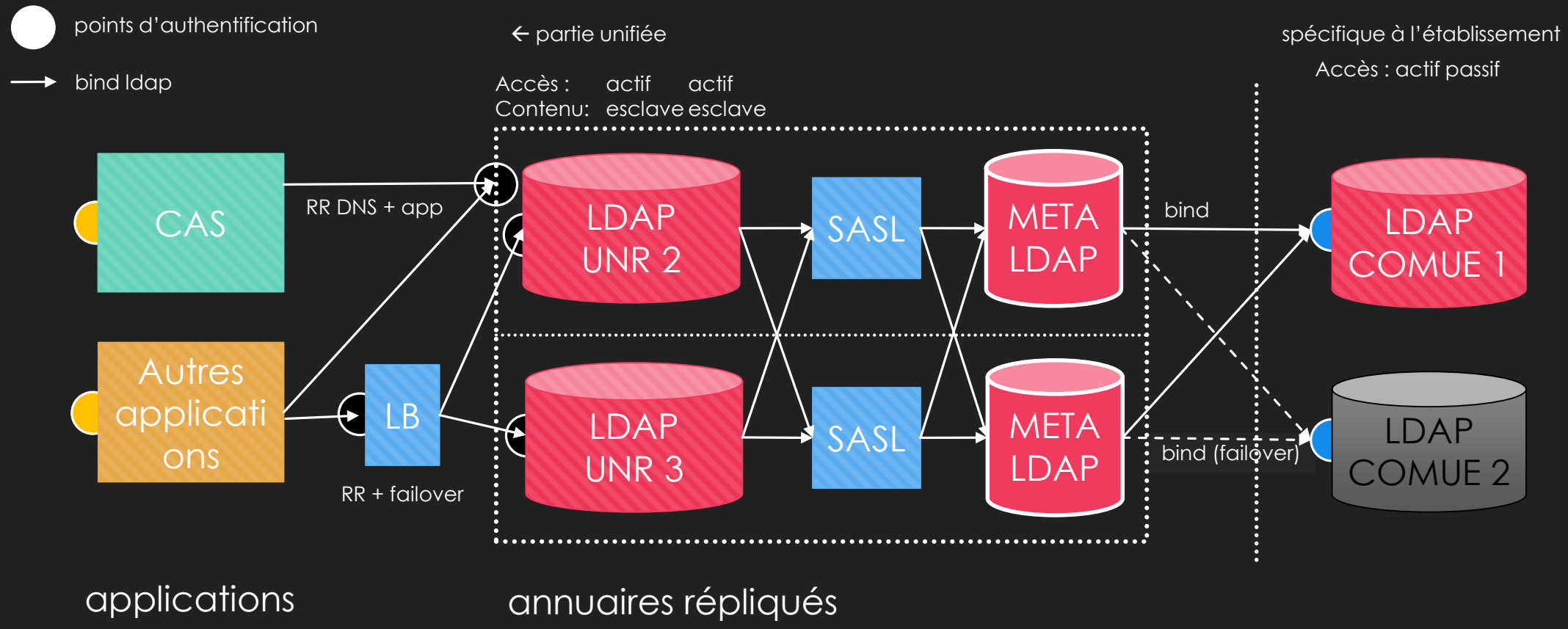
I - Annuaire et fédération d'identité (3)

- Fonctionnement du LDAP pass-through
  - Champ userPassword détermine la destination
  - Format des identifiants



I - Annuaire et fédération d'identité (4)

- Annuaire – architecture HA détaillée

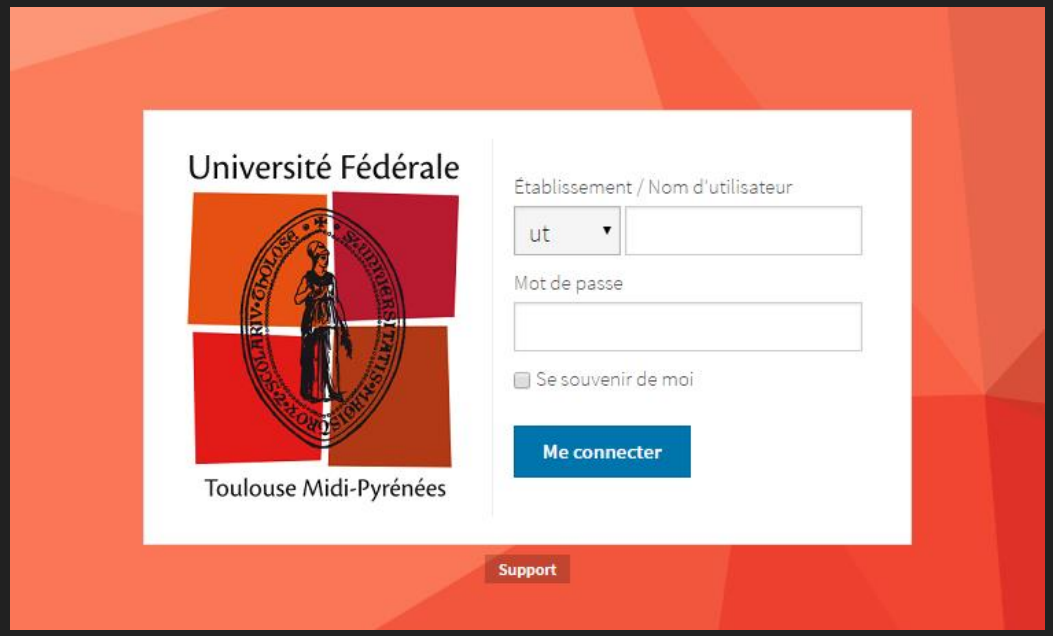


I - Annuaire et fédération d'identité (5)

- Performances du mécanisme pass-through
  - Conditions du test (hors architecture matérielle)
    - LDAP avec 100 000 entrées générées aléatoirement
    - LDAP établissement : UT2
    - Connexions (bind) sur des entrées aléatoires
  - 1 chaine complète d'authentification : ~ 7,5ms ➔ ~ 133 connexions / s
  - Variable la plus importante : connexion Cloud UNR ⇔ Etablissement

Plan

- Introduction : une évolution nécessaire
- I – Annuaire LDAP unifié, fédération d'identité
- **II – Du CAS Apereo au CAS Casino**
- III – Évolutions du CAS
- IV – Architecture finale, haute disponibilité
- V – Vers la fédération d'identité Shibboleth
- Conclusion



II - Du CAS Apereo au CAS CASino (1)

- CAS Jasig/Apereo
  - Difficile à maintenir, à (re)déployer
  - Problèmes de sécurité (mises à jour Java)
  - Consommateur de ressources (Tomcat)

- Peut-on faire mieux ?

II - Du CAS Apereo au CAS CASino (2)

Université Fédérale
Toulouse Midi-Pyrénées

- CASino
  - Ruby on Rails (interprété, moderne, lisible)
  - Open Source (licence MIT)
  - Supporte CAS v1 & v2 + Single Sign Out
  - Fiabilisé (> 95% code testé / Travis / Specs Ruby)
  - Intégrable facilement dans une infrastructure HA
    - Stockage SQL
    - Respect standard des en-tête HTTP reverse-proxy
  - « clean code base »

II - Du CAS Apereo au CAS CASino (3)

Université Fédérale
Toulouse Midi-Pyrénées

- Bonus
  - Authentification deux facteurs / OTP
  - Affichage des sessions utilisateur

Hello!

CASINO

You are currently logged in as **john@example.com**.

Logout

Two-factor authentication

Currently enabled - **Disable**

Your Active Sessions

Browser	Services	Most recent activity	
Chrome (Macintosh)	0	less than a minute ago	**Current session**
Firefox (Macintosh)	1	4 days ago	**End session**
Chrome (Macintosh)	6	4 days ago	**End session**
Chrome (Macintosh)	2	10 days ago	**End session**

Set up two-factor authentication

Tow-factor authentication requires you to enter an additional one-time password (OTP) each time you try to login to your account. An OTP can be created with an application such as the **Google Authenticator** with your mobile phone.

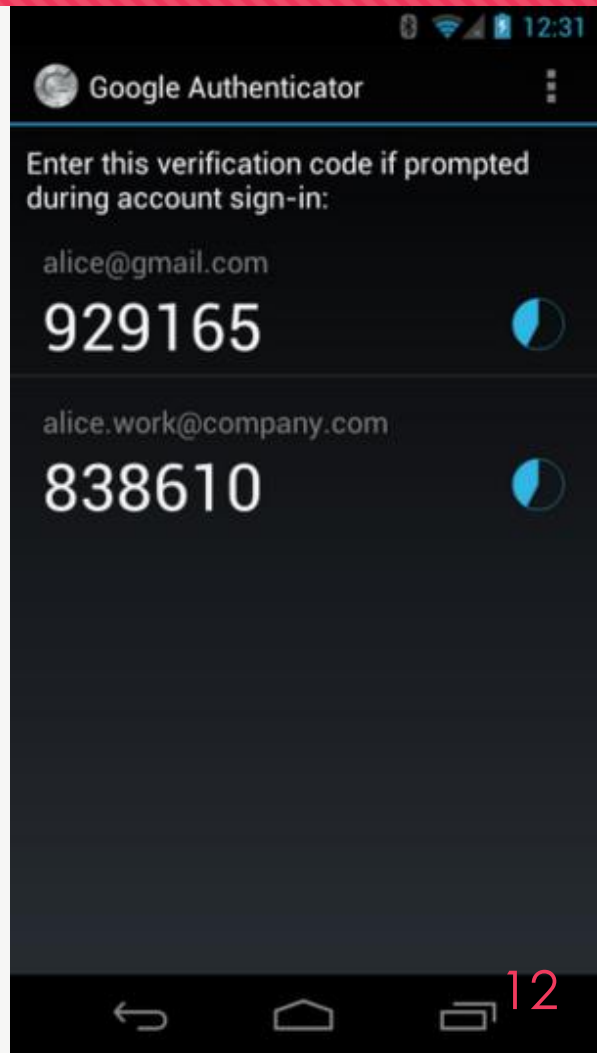
If you are using Google Authenticator, scan the QR code below with the application. Enter the verification code in the text field below.

Secret: o5xvl7tgs556lbc4

Confirmation code

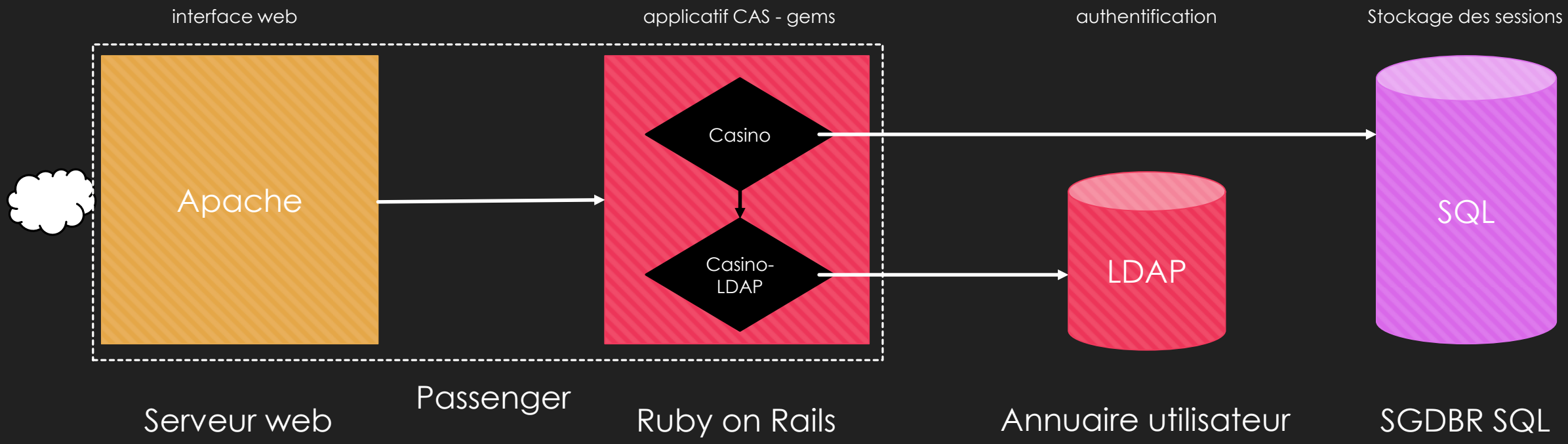
Cancel **Verify and enable**

Powered by **CASino**



II - Du CAS Apereo au CAS CASino (4)

- Architecture logique CASIno

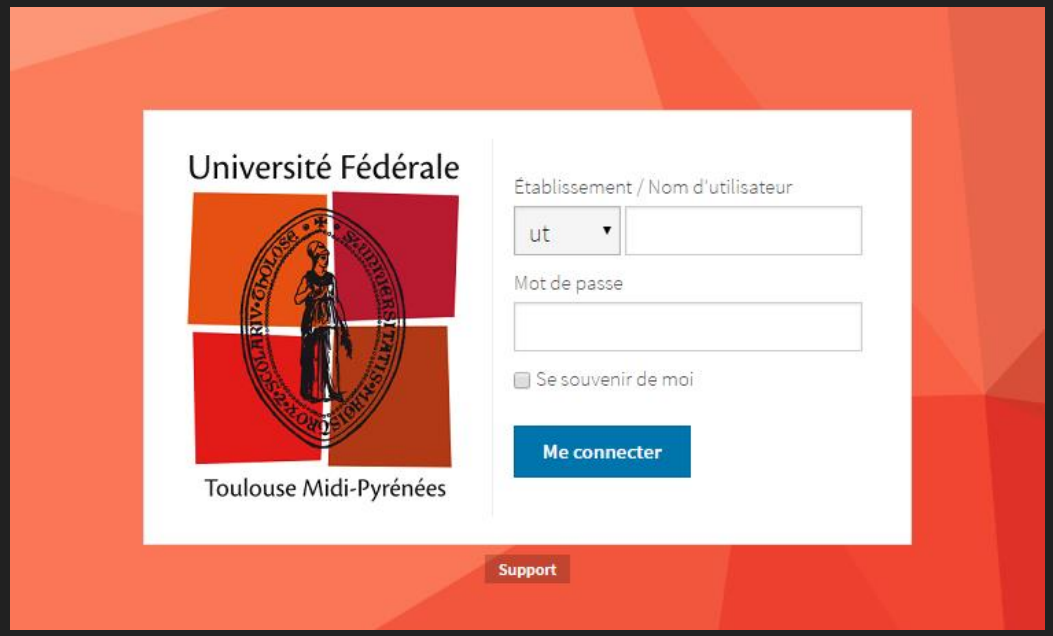


II - Du CAS Apereo au CAS CASino (6)

- Bilan
  - Les +
    - Simplicité de l'architecture
    - HA
      - Fournir deux serveurs CASino
      - Fiabiliser le backend SQL
    - Évolutivité (Open Source)
  - Les -
    - non support de protocoles récents (CAS v3 / SAML, OpenID.. CASShib)
      - est-ce vraiment utile ?
    - peu de retours d'utilisateurs

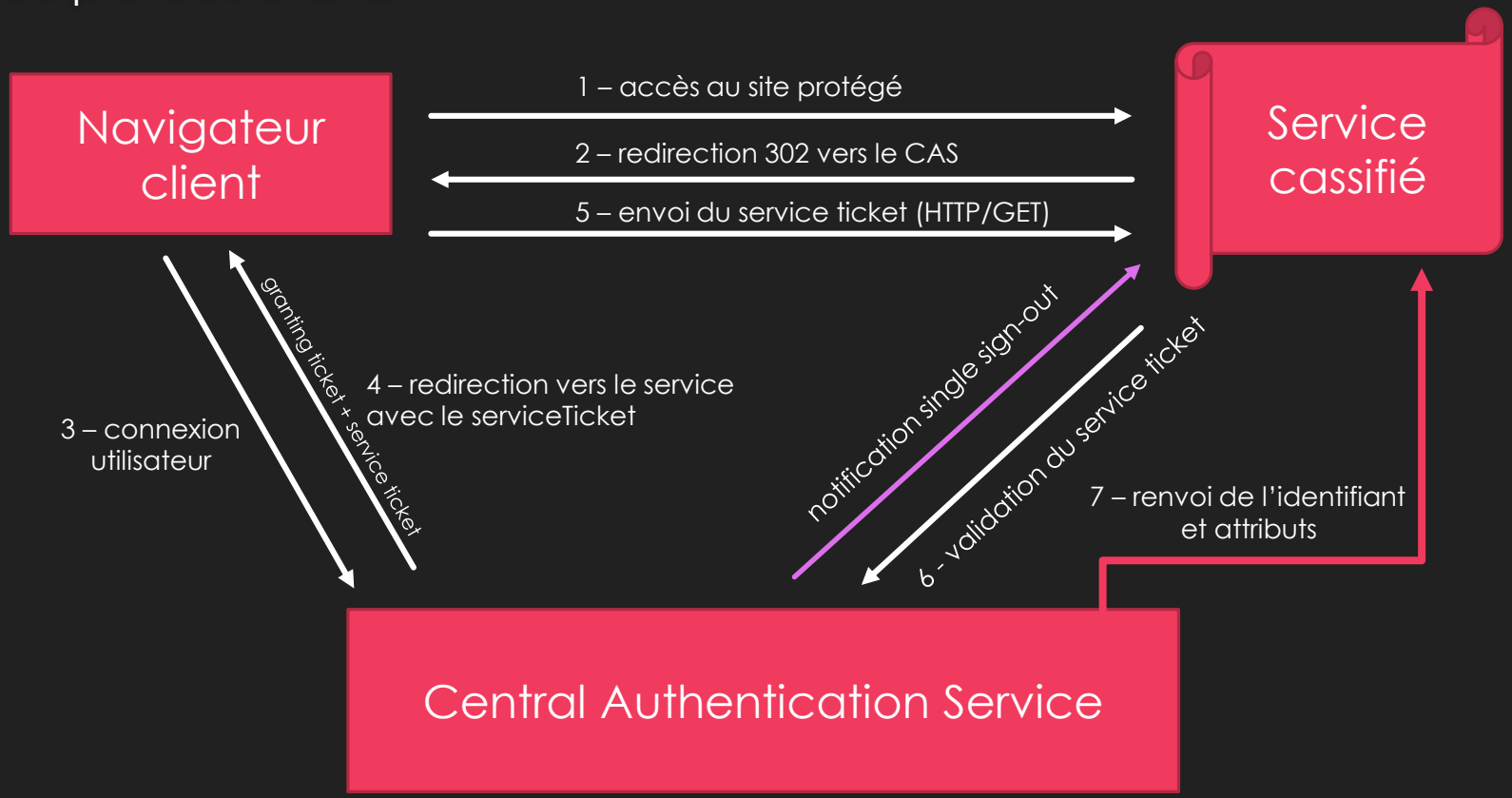
Plan

- Introduction : une évolution nécessaire
- I – Annuaire LDAP unifié, fédération d'identité
- II – Du CAS Apereo au CAS Casino
- **III – Évolutions du CAS**
- IV – Architecture finale, haute disponibilité
- V – Vers la fédération d'identité Shibboleth
- Conclusion



III – Évolution du CAS (1)

- Rappel du protocole CAS



III – Évolution du CAS (2)

- Rappel du protocole CAS (suite)
  - 1 service = 1 URL (regex)
  - Exemple : Service de gestion des commandes de café (application web)
    - URL : https://gestion-café.univ-toulouse.fr

III – Évolution du CAS (3)

Université Fédérale
Toulouse Midi-Pyrénées

- 1ère évolution: Ajout du contexte / service
  - Objectifs
    - Gérer identifiants locaux (établissement) / globaux (UNR)
    - Format de l'identifiant dépendant du service
    - Iso-fonctionnalité avec l'ancien CAS
  - Utilisateurs limités dans leur contexte (établissement)
  - ~ 200 lignes de codes modifiées (la moitié sur l'interface web)
  - Une semaine pour l'implémentation totale

III - Évolution du CAS (4)

Université Fédérale
Toulouse Midi-Pyrénées

- 2nd évolution: filtrage des services / groupe
  - Objectifs:
    - déporter le filtrage des utilisateurs en amont sur le serveur CAS
      - faciliter l'intégration des services
  - Groupes définis dans le LDAP (remontés par établissements)
  - En plus de filtre par établissement (contexte), on délivre des tickets sous certaines conditions
- Développement d'une interface de gestion des services

III – Évolution du CAS (5)

- Mise en application des deux évolutions
  - Pour un compte multi-établissement:
    - Identifiant établissement ut → jdoe (prioritaire)
    - Identifiant établissement ut2 → john.doe
    - Groupe: _ut2_etudiants

Entrée LDAP UNR

dn: ut.jdoe,ou=people,dc=unr,dc=fr
uid: ut.jdoe
cn: John Doe
unrID: jdoe@UT
unrID: john.doe@UT2
unrID: ut.jdoe@UNR

Nom du service	URI du service	Contexte	Groupe(s)	Identifiant retourné
Service COMUE	https://servivce-comue.fr/.*	ut		jdoe
Service COMUE accessible aux admins	https://admin-comue.fr.*	ut	_ut_admin	erreur
Service UNR	https://servivce-unr.fr/.*	unr		ut.jdoe
Service UT2	https://servivce-ut2.fr/.*	ut2	_ut2_etudiants	john.doe

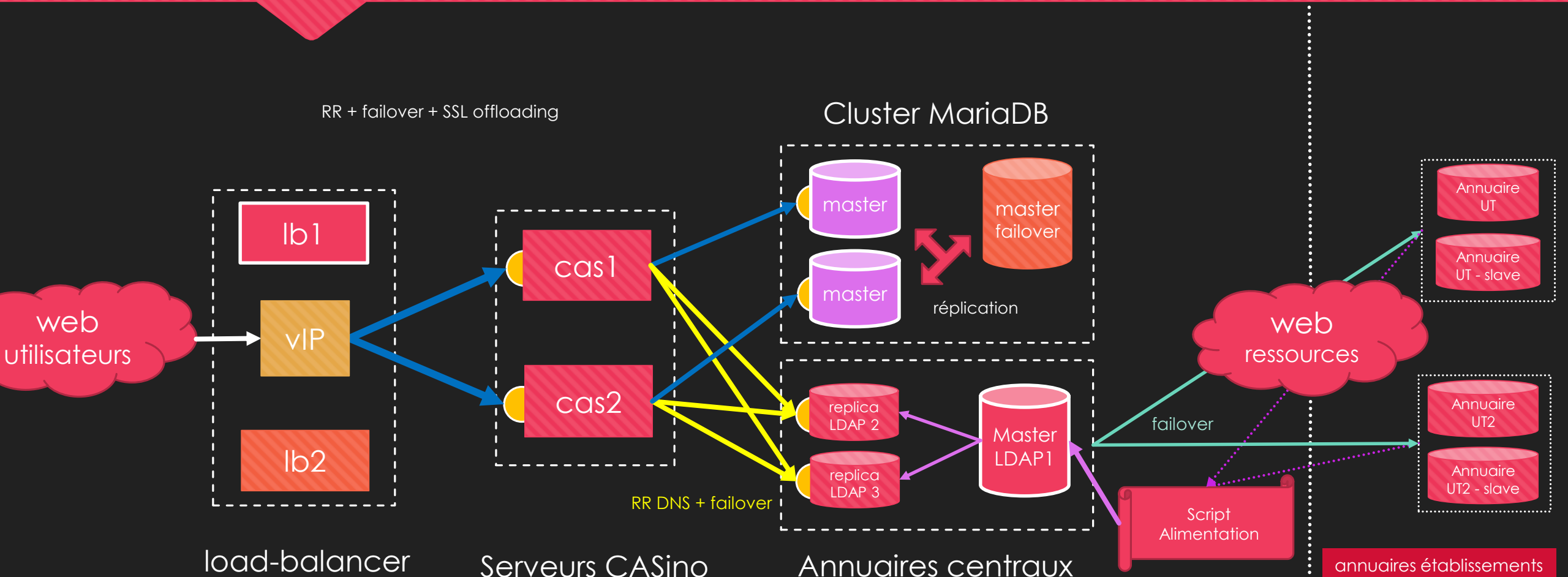
III – Évolution du CAS (6)

- Intégration client
  - Remontée générale de nouveaux attributs (mail, unrID, groupes)
  - Apache / mod_auth_cas
    - Patch
    - Lecture et filtrage attributs
  - phpCAS
  - Autres
    - Filtrage serveur

Plan

- Introduction : une évolution nécessaire
- I – Annuaire LDAP unifié, fédération d'identité
- II – Du CAS Apereo au CAS Casino
- III – Évolutions du CAS
- **IV – Architecture finale, haute disponibilité**
- V – Vers la fédération d'identité Shibboleth
- Conclusion

IV – Architecture finale, HA (1)



IV – Architecture finale, HA (3)

- Architecture totalement redondée
  - Pas de point critique (SPOF)
    - Faiblesses sur le script de génération de l'annuaire (beaucoup de traitements de données)
    - Cluster MariaDB Galera
      - Mode multi-master (tous peuvent écrire
      - Cause des erreurs 500 (deadlocks)
  - Parc de serveurs industrialisé
    - Puppet
    - Mises à jour automatiques & déploiement
      - Pas de technologie propriétaire
      - Reboot possible en production
    - Très peu coûteux (humain)
  - Évolution par composant

IV – Architecture finale, HA (4)

- Ressources consommées
  - LDAP => 3x (800M + 2vCPU)
  - CAS => 2x (1G + 1vCPU)
  - MariaDB => 2x (8G + 3vCPU) + 1x (4G + 3vCPU) => autres usages

- Comment intégrer le socle d'authentification ?
  - Vous êtes un établissement d'enseignement supérieur
  - Fournir un point d'authentification LDAP et remonter des fichier LDIF (document de spécification)

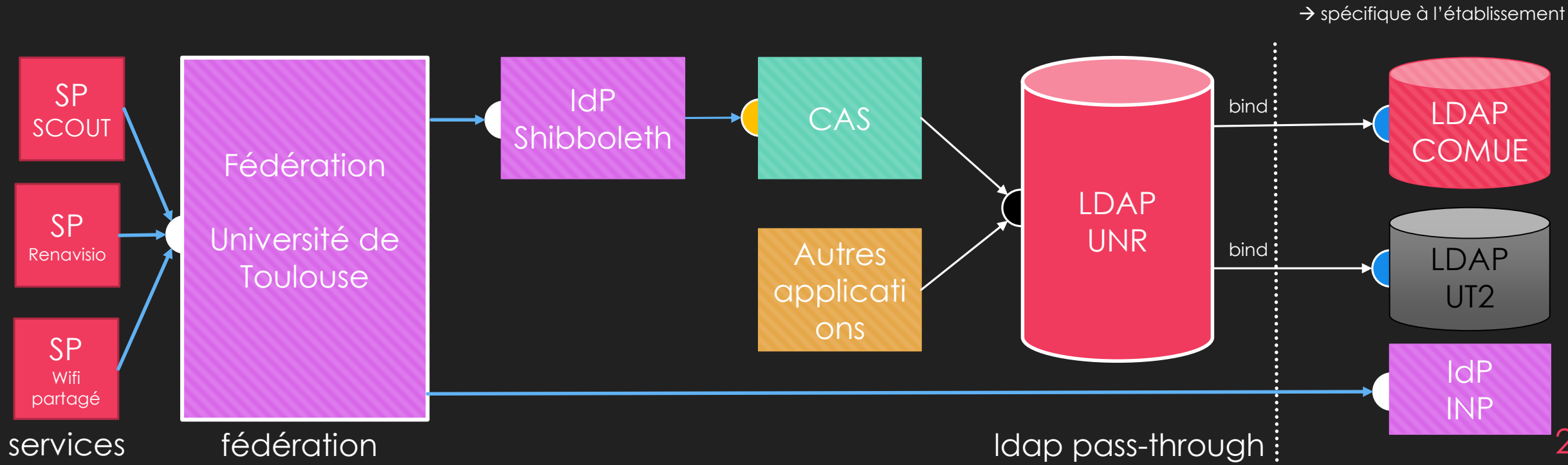
- Comment utiliser notre socle d'authentification ?
  - Services à valider individuellement sur le CAS (pas d'accès public)
  - Accès sur demande sépcifique au LDAP
  - Demandes & support sur support-cas_ldap@univ-toulouse.fr

Plan

- Introduction : une évolution nécessaire
- I – Annuaire LDAP unifié, fédération d'identité
- II – Du CAS Apereo au CAS Casino
- III – Évolutions du CAS
- IV – Architecture finale, haute disponibilité
- **V – Vers la fédération d'identité Shibboleth**
- Conclusion

V – Vers une fédération Shibboleth (1)

- Objectifs
  - Les établissements gèrent eux-mêmes leur circuit d'authentification
  - Fourniture d'un IdP pour les établissements qui n'en ont pas



V – Vers une fédération Shibboleth (2)

- Autres avantages
  - Utilisé dans les établissements publics, au niveau national
  - Shibboleth v3 est multi-protocolaire : Shibboleth/SAML + CASv2
- Travail en cours
  - fin de support de la v2 → passage en v3 nécessaire
  - Intégration des établissements dans la fédération UFTMiP
  - Nombreux questionnements « usages »
    - Single Sign-Out
    - Full SSO => Auto-sélection de l'IdP lorsque l'utilisateur est connecté
    - Inter-opérabilité et intégration
  - Conversion des services CAS → Shibboleth

Conclusion

- Bilan technique / d'exploitation
  - CAS mis en place le 22 septembre
    - Aucun problème spécifique à CASino rencontré
    - Cluster MariaDB
  - LDAP
    - Déjà utilisé par le CAS et pour le routage mail
    - Synchronisation efficace
    - Bascule efficace lorsqu'un LDAP ne répond pas
- Bilan humain, coût d'exploitation
  - Fork COMUE à maintenir
- Contribution Open Source et licence


Université Fédérale
Toulouse Midi-Pyrénées
Établissement / Nom d'utilisateur
ut
Mot de passe
Se souvenir de moi
Me connecter
Support

Compte non autorisé

Vous ne pouvez pas accéder à ce service "**https://commande-café.univ-toulouse.fr/**" qui requiert le(s) groupe(s) **cafémanager** avec ce compte **ut.jeboisduthé**.

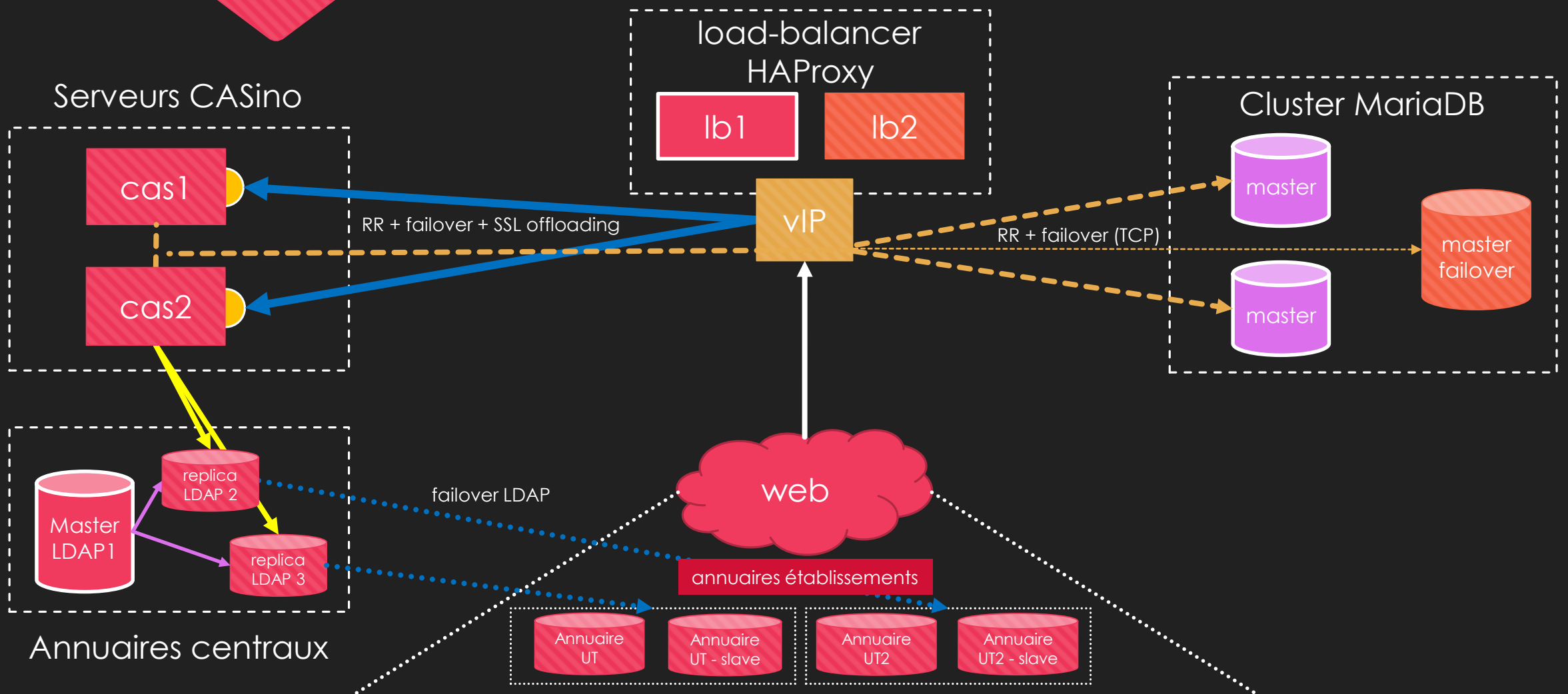
Profil - Se connecter avec un nouveau compte

Université Fédérale

Toulouse Midi-Pyrénées

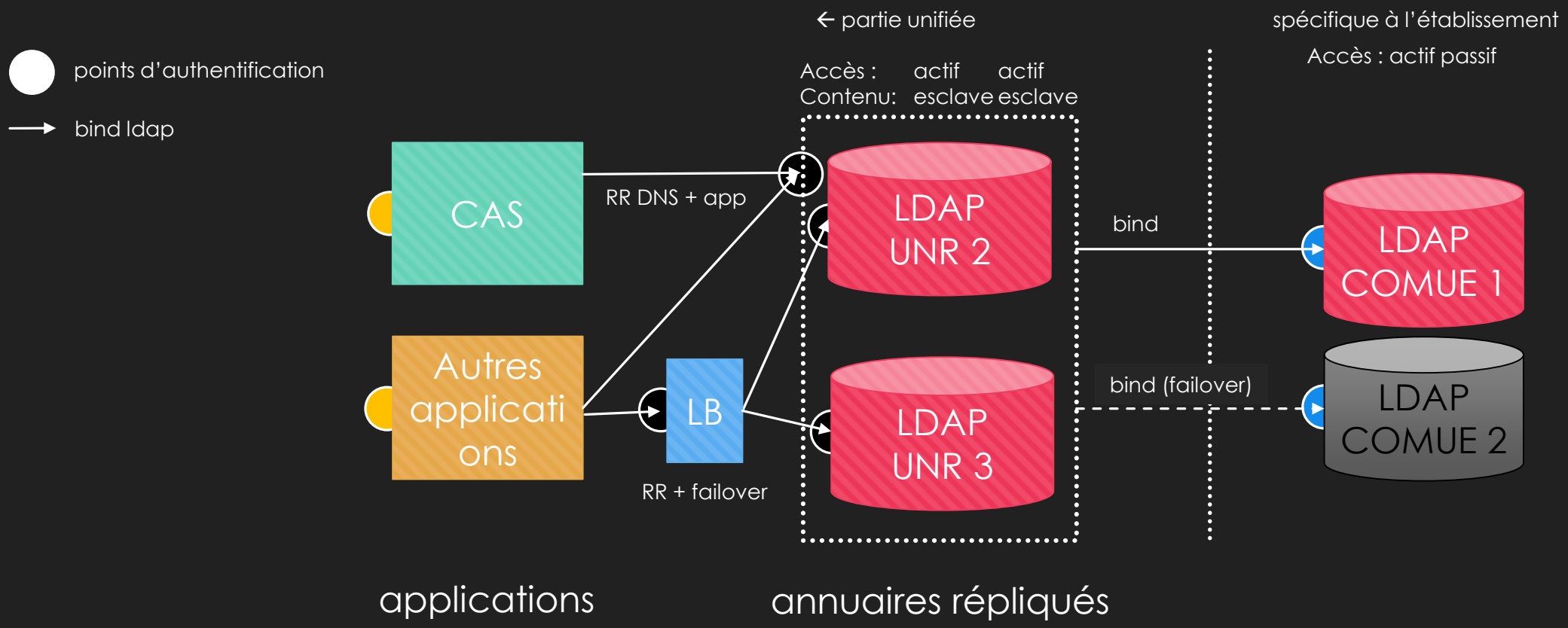
Support

Architecture finale w/ LB DB



I - Annuaire et fédération d'identité

- Annuaire – architecture HA



I - Annuaire et fédération d'identité

- Fonctionnement du pass-through
  - Champ userPassword détermine la destination
  - Format des identifiants