Mise en place Télétravail et fonctionnement à EcoLab

CAPITOUL 14 février 2019

Hugues ALEXANDRE

Environnement unité

- UMR (CNRS, UPS, INPT)
  - 3 Sites interconnectés permanents
  - 1 AD unique
    - Gestion centralisée des postes de travail et cptes utilisateurs
  - Postes de travail
    - Compte usager AD sans droits « avec pouvoir » ou « administrateur »
    - Pas de compte local non AD
  - Parc
    - > 95% postes Windows

Historique des accès distants à EcoLab

Depuis 2008 (>10 ans)

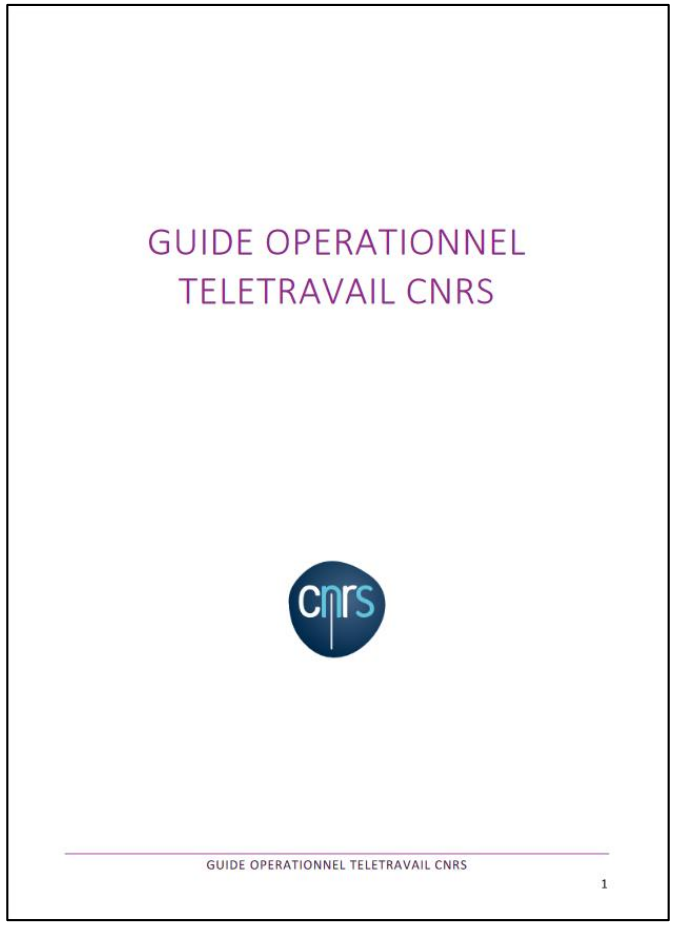
- VPN IPSec nomade
- VPN IPSec inter Appliances (toujours actif)
  - Interconnexions de sites
  - Permet l'interconnexion des réseaux privés et fonctionnement d'un AD multi sites

2018

- Arrêt VPN IPSec nomade
  - Coût licence client
  - Complexité lors de migration de machine
    - pour réinstaller, annulation licence sur ancien poste via l'assistance FW
  - Plus en plus bloqué par les organismes intermédiaires
- Remplacement par VPN SSL
  - Passe partout => utilisation du port 443
  - Client Stormshield => changement envisagé vers OpenVPN
  - Config FW authentification => AD
  - Authentification VPN SSL => Compte AD
  - Gestion des usagers télétravailleurs => via un groupe AD « Teletravailleurs »
    - ➢ Pas de changement sur FW si nouveau ou retrait statut télétravailleur > Chgt dans AD

Base réglementaire

- Guide opérationnel télétravail CNRS
  - https://intranet.cnrs.fr/delegations/dr8/actualites/Documents/go-teletravail-okpostct.pdf
  - Page 22 et pages 34 à 38
    - Sécurité des données et de l'équipement
    - L'accès distant et la sécurité du réseau
    - L'utilisation des NTIC
    - L'assistance distant


GUIDE OPERATIONNEL
TELETRAVAIL CNRS

GUIDE OPERATIONNEL TELETRAVAIL CNRS

1

Condition administrative pour le télétravail

- Document unique des risques professionnels => rempli par l'usager
- Avis du responsable => complété et signé
- Accord télétravailleur => DU
- Attestation conformité équipements NTIC => signé par CSSI
  - Equipement conforme aux règles laboratoires (chiffrement des disques, antivirus, machine intégré AD…)
- Conditions spécifiques unité demandé par le SI
  - Compte usager MyCore => actif
  - Compte usager MyCom => actif

Coût du poste de télétravailleur

- Equipement de base quotidien
  - Ordinateur portable (celui du quotidien)
- Coûts supplémentaires (250 €)
  - 1 écran 22’’ (130 €)
  - 1 station d’accueil (95 €)
  - 1 Clavier + souris (20 €)

Environnement travail usager

- Authentification
  - Code identique poste de travail, VPN, service accès distant
- Connexions VPNs
  - Installé et configuré par SI
- Accès Bureau Accès Distance (BAD)
  - Accès au(x) réseau(x) EcoLab et données serveur(s)
- Environnement de travail
  - Identique poste de travail / session accès distant

Configuration poste télétravailleur

- Service Bureau accès distant
  - Windows
    - Intégré (authentification session usager)
  - Macintosh
    - Intégré à la suite Office (utilisation Windows sur serveur distant)
- Client Owncloud
  - Configuré avec cpte usager MyCore
    - ➢ Compte RESEDA (configuré par usager ou SI)
- Skype entreprise
  - Configuré avec cpte usager MyCom
    - ➢ Compte RESEDA (configuré par usager ou SI)

Accès infra, données, impressions

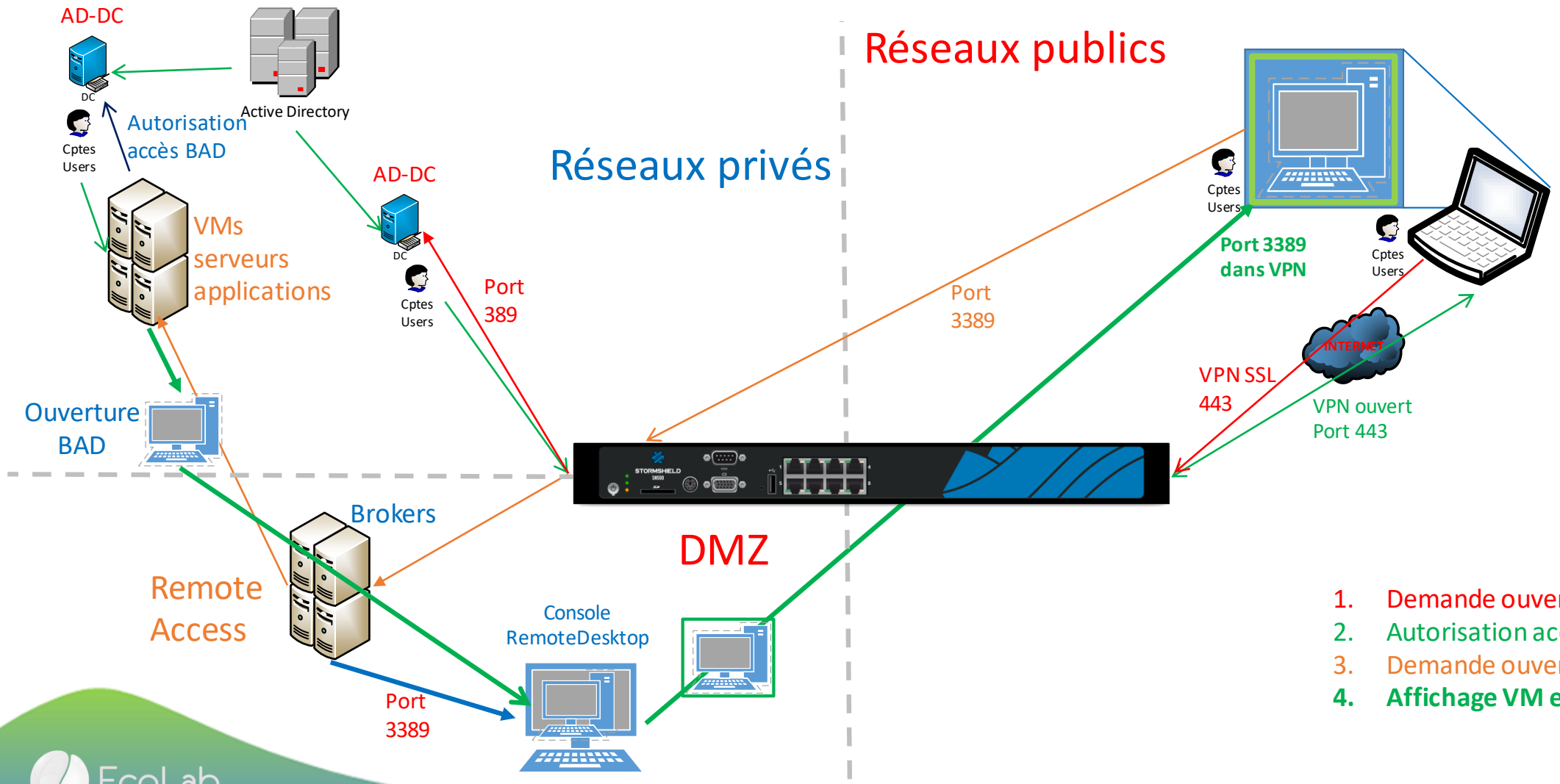
- Accès
  - Uniquement en BaD Windows (port 3389)
    - Un ou plus serveur(s) suivants droits (compte AD autorisé sur une ou plusieurs VM serveurs)
- Environnement usager
  - Même profil usager et télétravailleur (imprimantes, partages réseau)
    - 4 partages montés sous forme de disques réseaux par GPO
      - Partage personnel
      - Partage équipe
      - Partage labo
      - Partage toolsbox
  - Imprimante personnel maison accessible sur session BaD
  - Sauvegarde automatique données local Atempo ALN
  - Echange/sauvegarde => Client Owncloud (compte MyCore)

Avantages pour SI

- Gestion des incidents
  - Simplification de gestion et d'assistance
    - Même procédure d'accès distant pour nomadisme et télétravailleur
- Sécurité des accès
  - Simplification et sécurité accrue (limitation ouverture de ports réseaux ouverts)
    - 443 (VPN SSL) entre poste et FW
    - 3389 (Remote Desktop) accès serveur et échange poste de travail
- Sécurité virale
  - Antivirus gérés par un serveur d'administration et droits restreints pour le client
    - Client antivirus sur serveur
    - Client antivirus sur poste travail
- Garantie SI
  - Niveau de sécurité
    - Identique sur un serveur ou sur ordi professionnel
  - Si un ordi non professionnel
    - Sécurité garantie coté serveur

Fonctionnement et config

La connexion et mise en place du télétravail



1. Demande ouverture du VPN SLL
2. Autorisation accès VPN validé
3. Demande ouverture Remote Desktop
4. **Affichage VM et travail à distance**

EcoLab

Config FW

Config LDAP

CONFIGURATION DES ANNUAIRES

ANNUAIRES CONFIGURÉS (5 MAXIMUM)

Ajouter un annuaire | Action

Domain name

CONFIGURATION | STRUCTURE

Annuaire distant

Activer l'utilisation de l'annuaire utilisateur

Serveur: serv

Port: ldap

Domaine racine (Base Dn): dc=

Identifiant: cn=administrateur,

Mot de passe:

DROITS D'ACCÈS

ACCÈS PAR DÉFAUT | ACCÈS DÉTAILLÉ | SERVEUR PPTP

Rechercher... | Ajouter | Supprimer | Monter | Descendre

	Etat	Utilisateur - groupe d'utilisateurs	VPN SSL Portail	IPSEC	VPN SSL	Parrainage	Description
7	Activé	ECOLAB Teletravailleurs@ecolog-in	Autoriser	Interdire	Autoriser	Interdire	

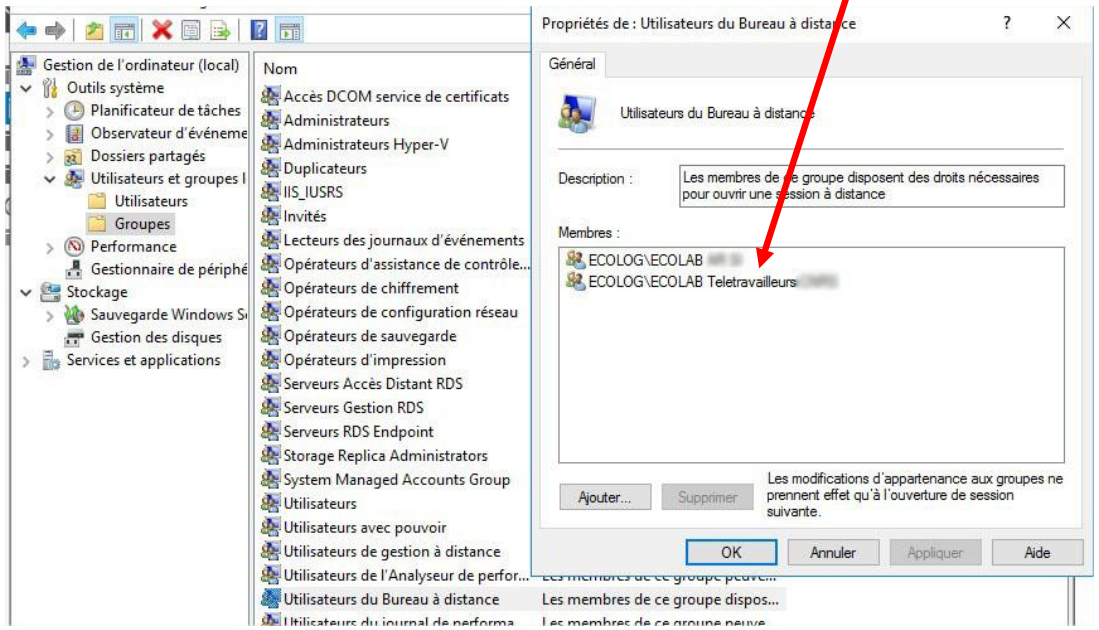
contient 8 règles, de n° 7 à n° 14)

on	passer	Reseau_VPN-SSL	serv- serv-	domain_udp domain	IPS	Resolution DNS interne
on	passer	ECOLAB Teletravailleurs via Tunnel VPN SSL	GRP_Machines_Teletravail	microsoft-ts	IPS	Acces télétravail
on	passer	ECOLAB via Tunnel VPN SSL	GRP_ GRP_	microsoft-ts	IPS	Accès avec compte Admin SI
on	passer	ECOLAB via Tunnel VPN SSL	GRP_	microsoft-ts	IPS	Accès gestion financiere
on	passer	ECOLAB via Tunnel VPN SSL	GRP_	microsoft-ts	IPS	Accès direction
on	passer	ECOLAB via Tunnel VPN SSL	GRP_	microsoft-ts	IPS	Acces Modélisation CC et CV
on	passer	ECOLAB via Tunnel VPN SSL		GRP_SRVC_MICROSOF	IPS	Acces serv tech SI accès serveur data

Config serveurs
Sur serveur accès distant

Ajouter les rôles des services bureau à distant en retirant le service Broker

Ajouter des groupes d'usagers télétravailleur dans le groupe « Utilisateur bureau à distance »

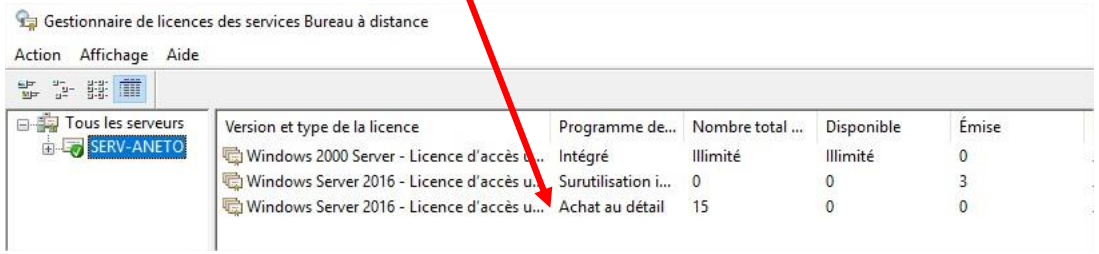


EcoLab

Config serveurs
Sur serveur de licences des services BaD

Ajouter les rôles des services bureau à distant en retirant le service Broker

Ajouter les CALLS suffisantes pour le télétravail

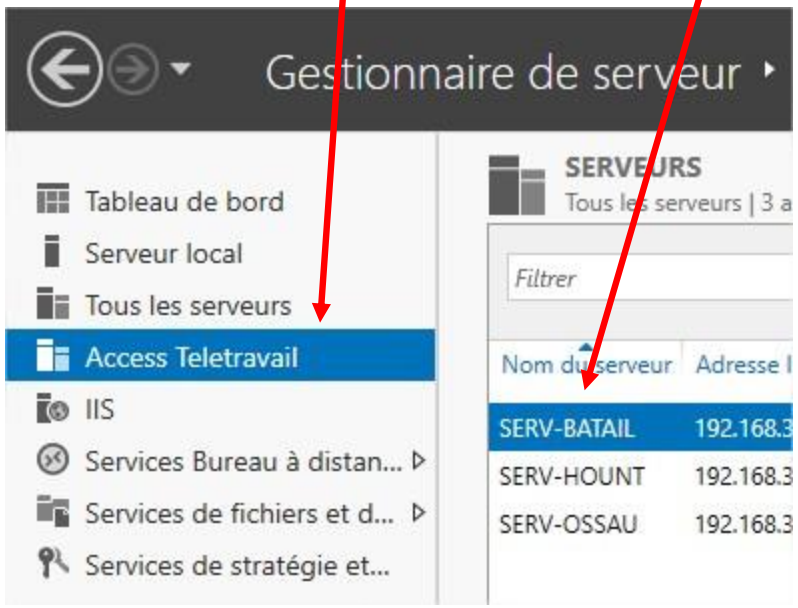


EcoLab

Config serveurs
Service broker

Ajouter les rôles des services bureau à distant et configurer le broker

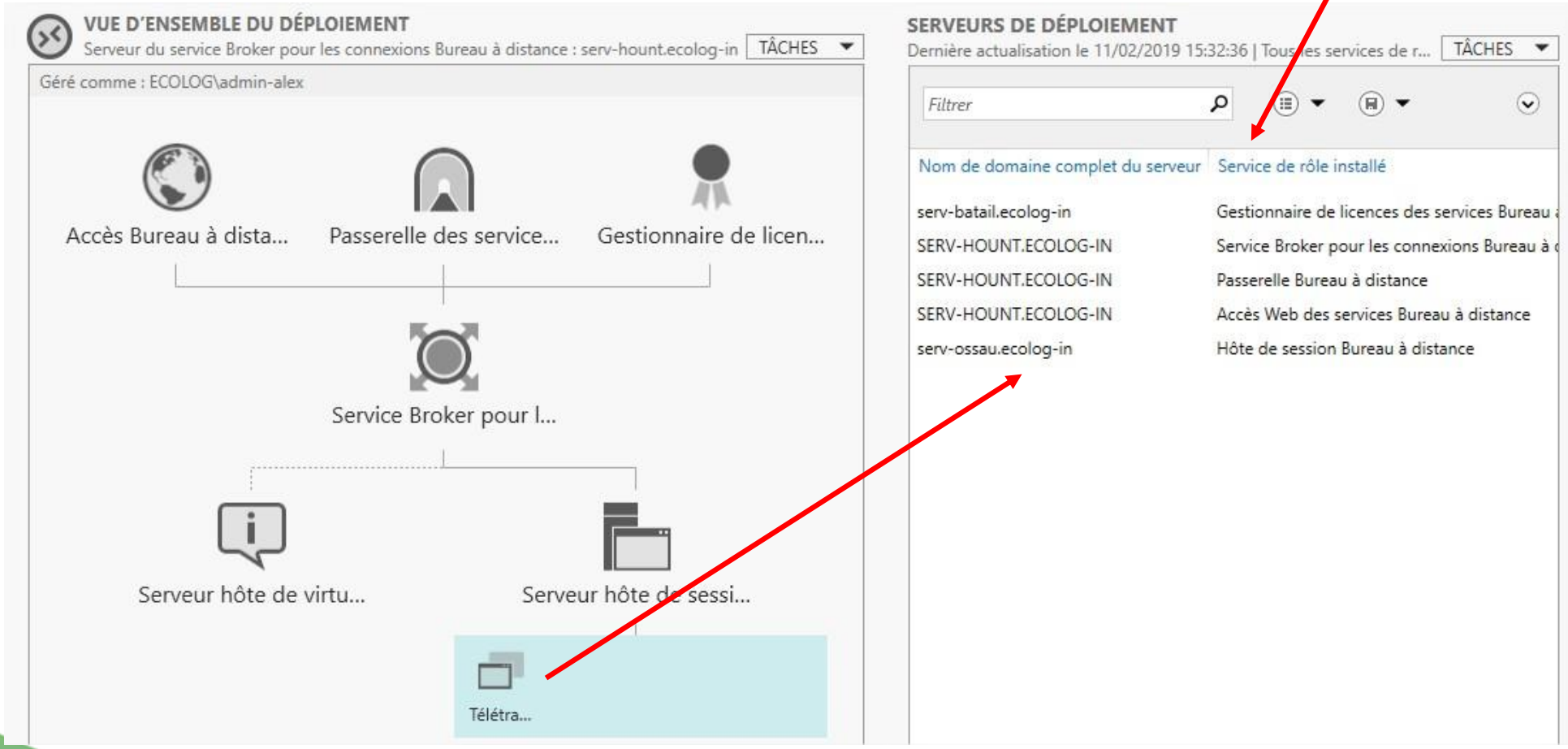
Créer le groupe des serveurs et affecter les serveurs concernés



EcoLab

Config serveur
Service broker

Affecter les rôles des serveurs au groupe créé

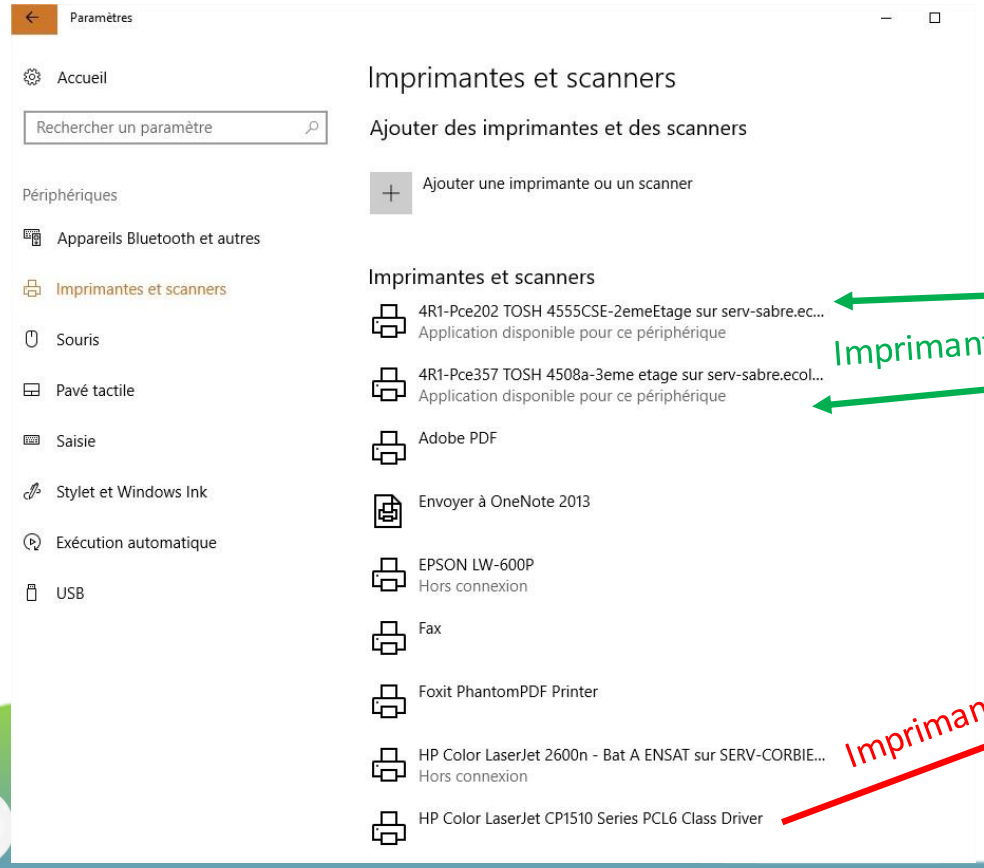


EcoLab

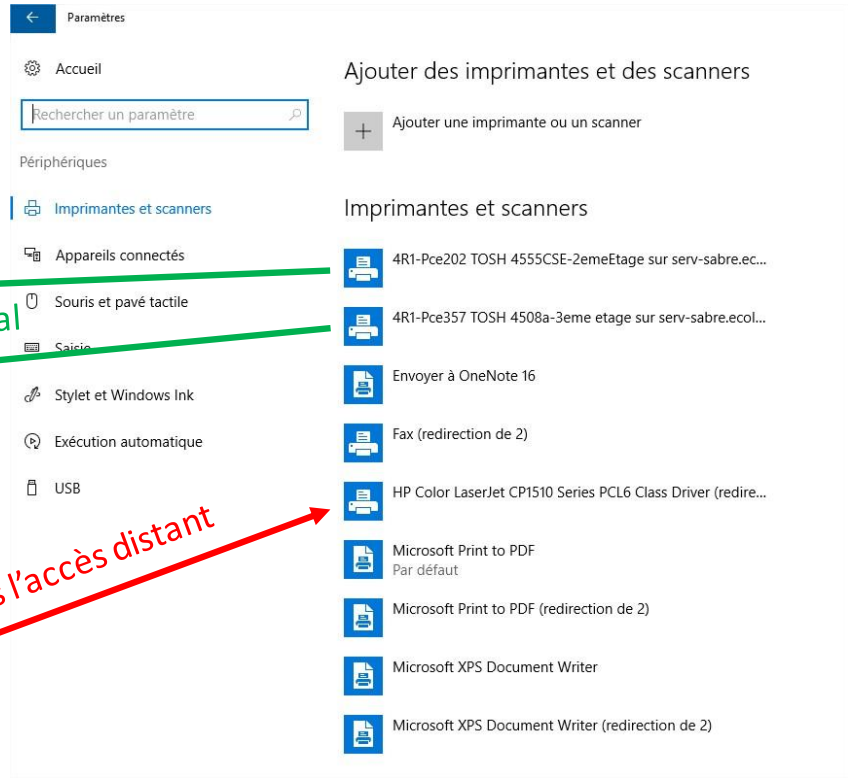
Environnement de travail

Environnement impression

Poste de travail



Session à distance

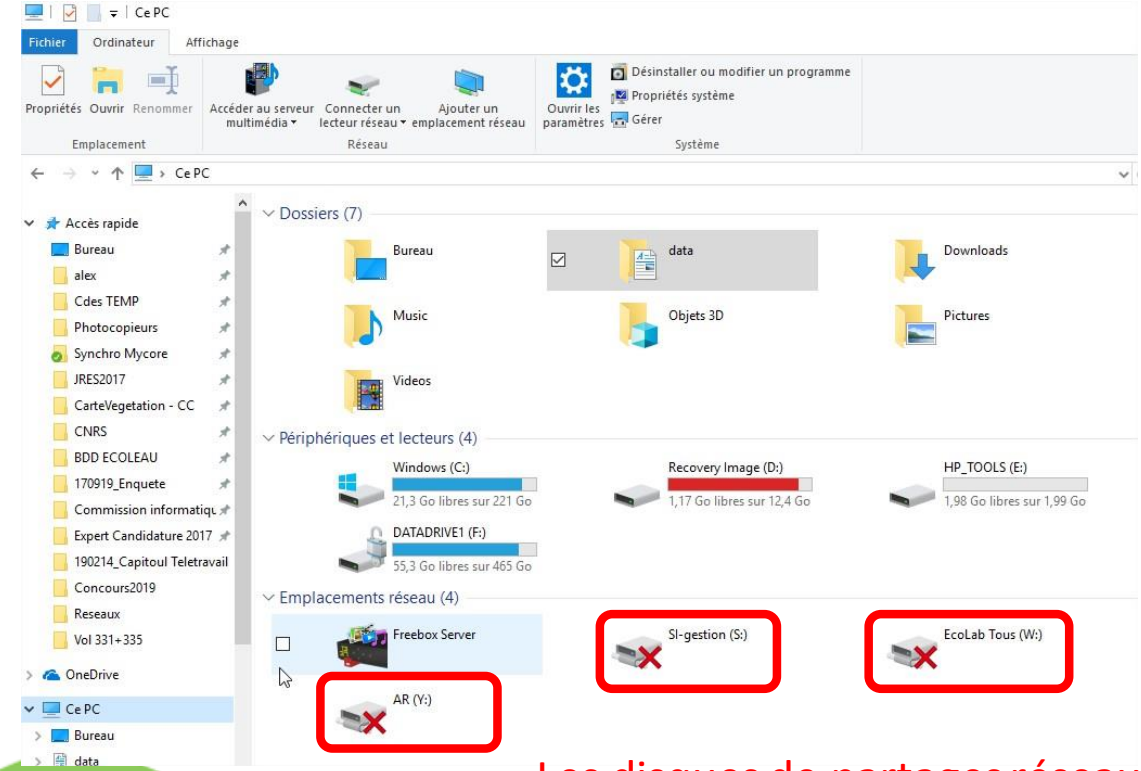


Imprimante labo active en local

Imprimante maison active dans l'accès distant

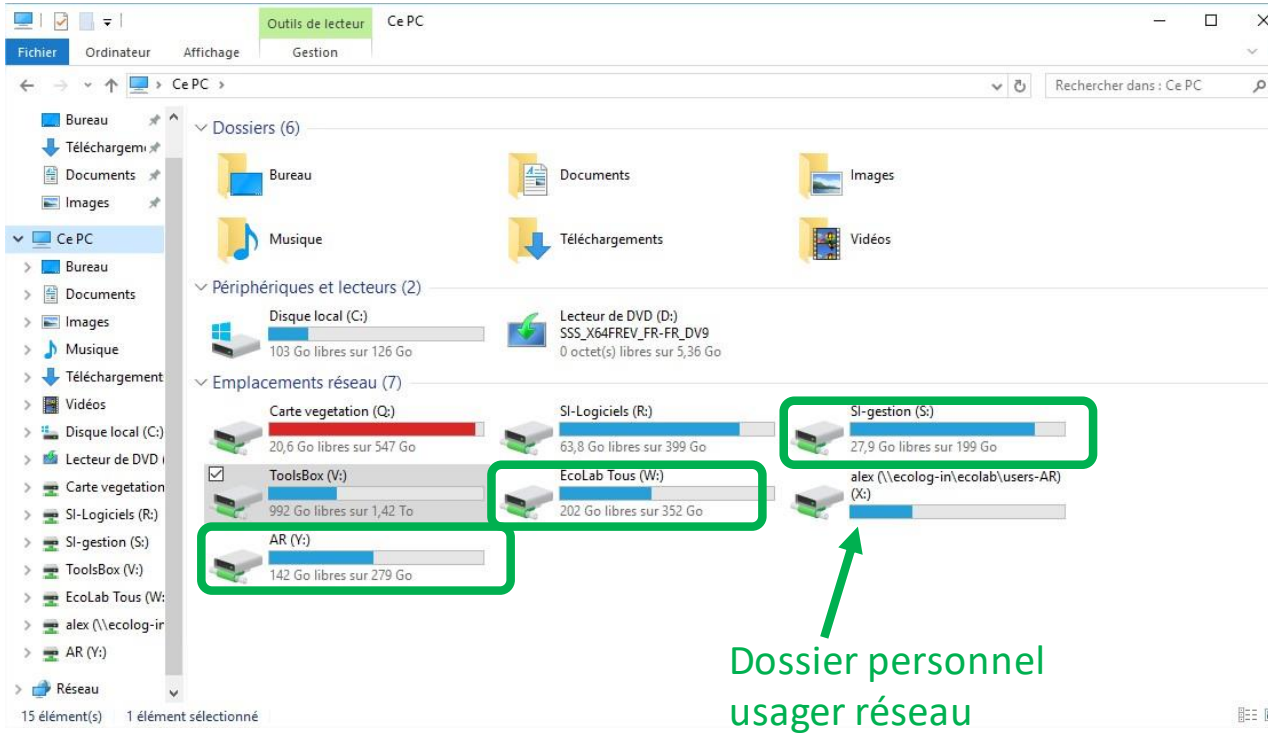
Echange de fichiers

Poste de travail état télétravailleur



Les disques de partages réseaux EcoLab ne sont pas accessible

Session à distance



Dossier personnel usager réseau

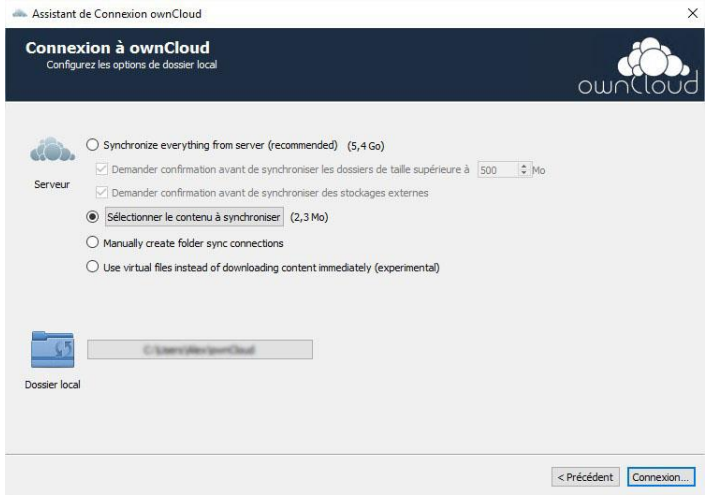
EcoLab

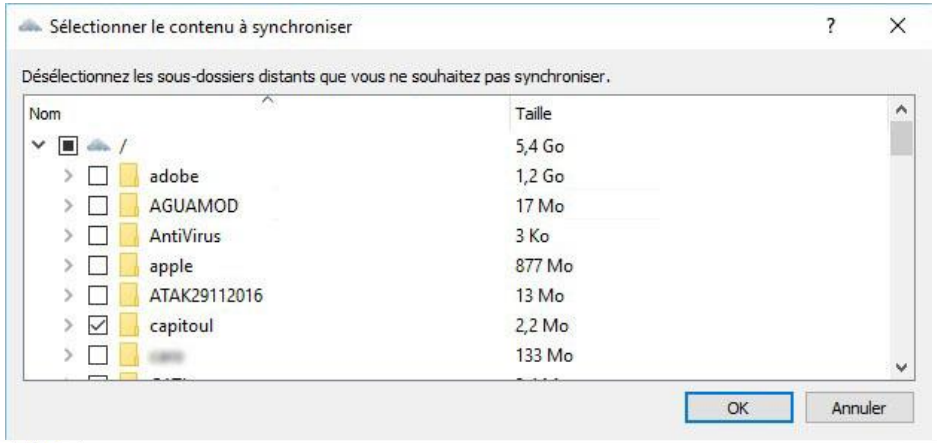
Echange de fichiers

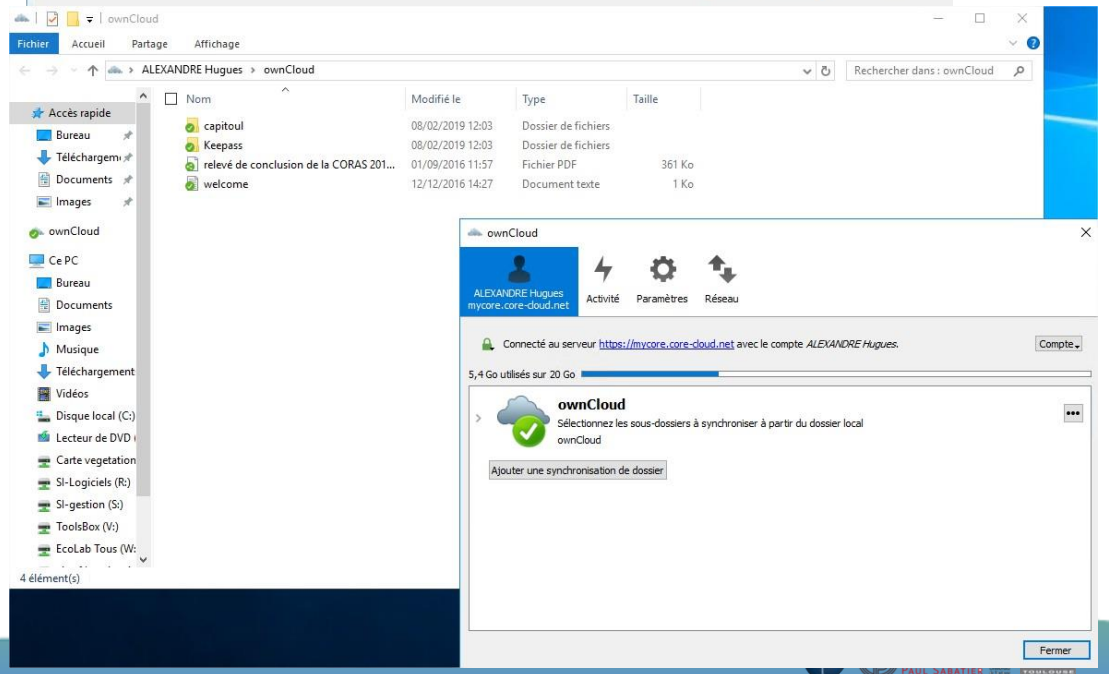
- Solution 1
  - Copier / coller
    - poste de travail ⇔ session distante

Echange de fichiers

- Solution 2
  - MyCore
    - Client Owncloud sur le serveur et sur le poste de travail



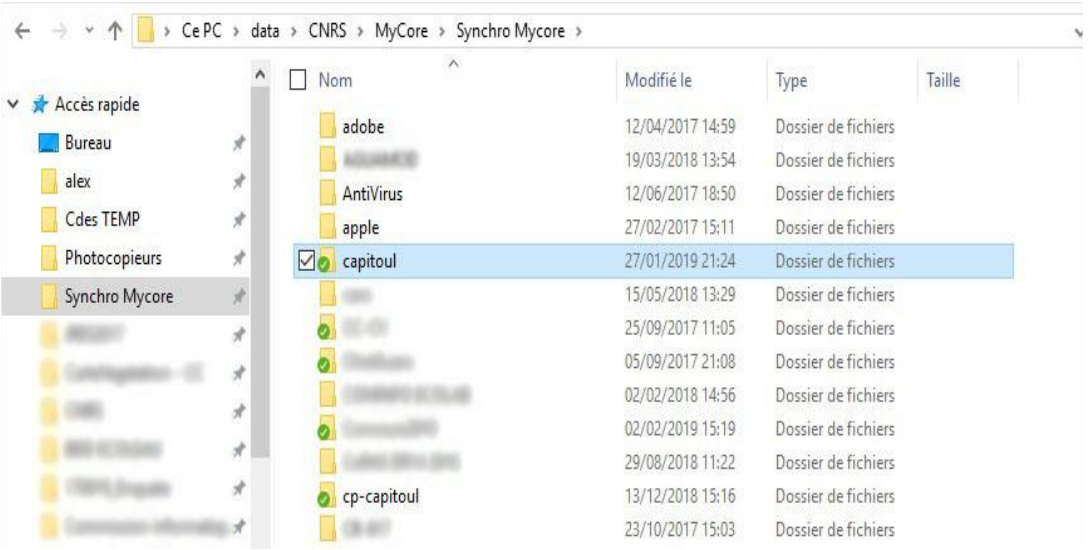




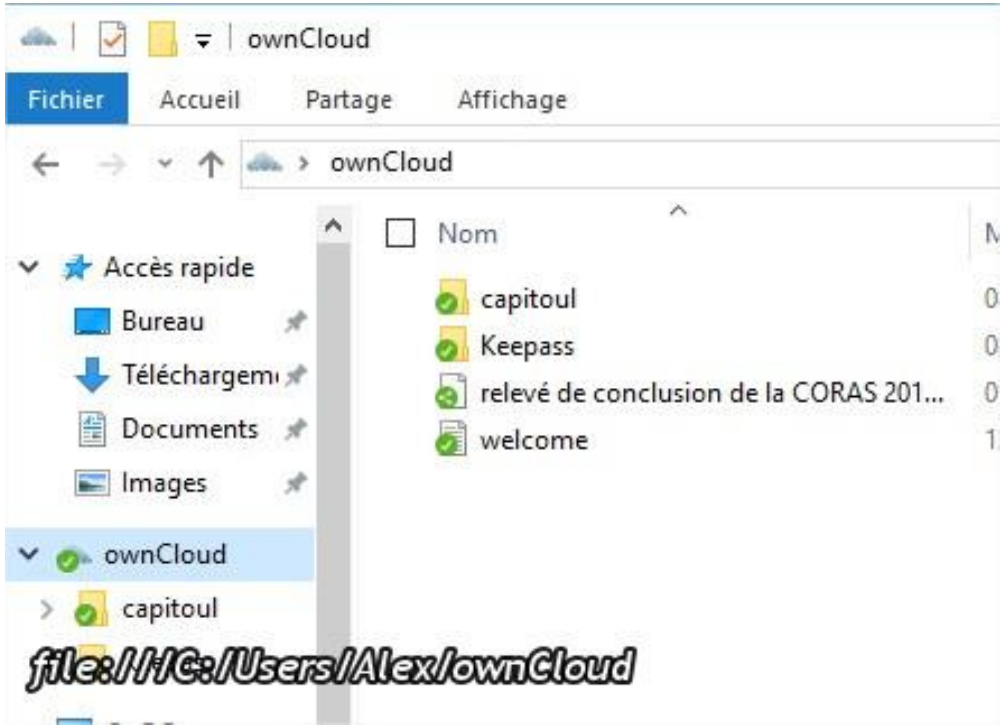
EcoLab

Echange de fichiers

Poste de travail

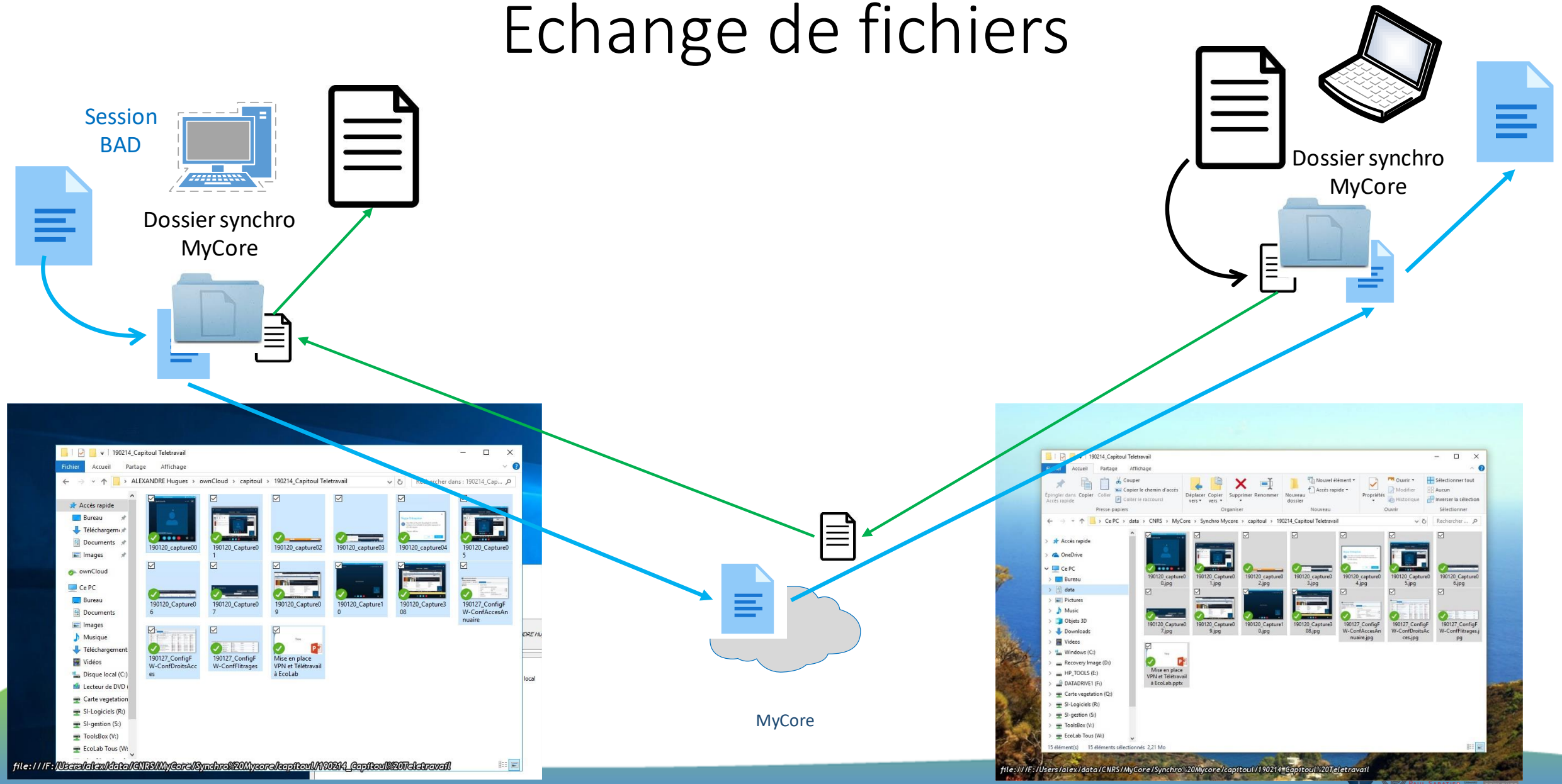


Session à distance



EcoLab

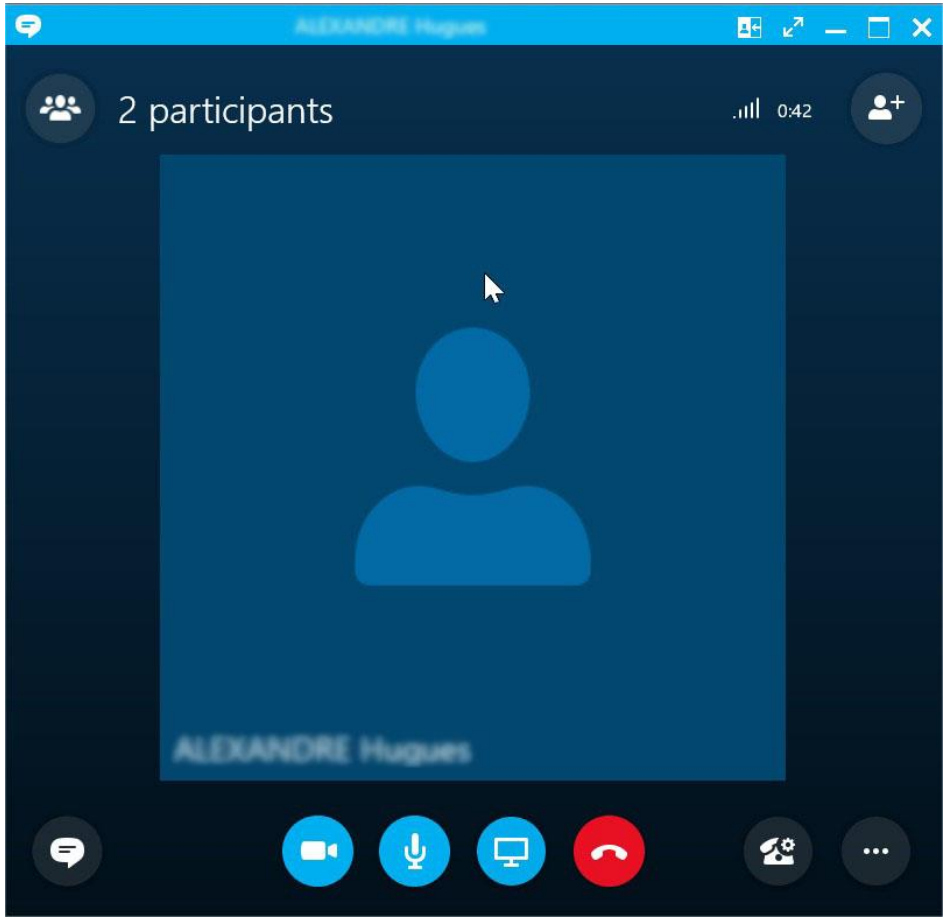
Echange de fichiers



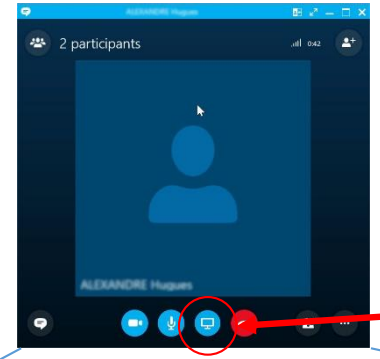
Assistance distante

Assistance distante

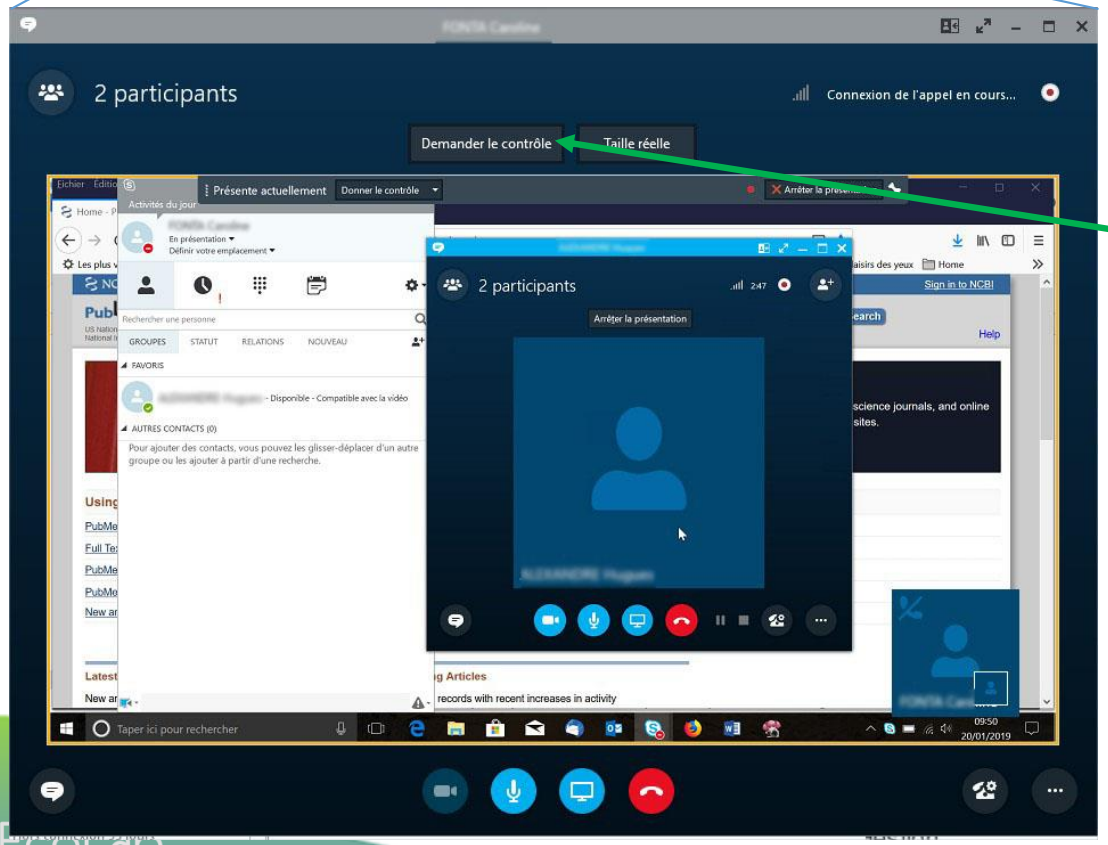
- Utilisation de MyCom
  - Téléphonie
  - Chat
  - Prise en main à distance



Assistance distante



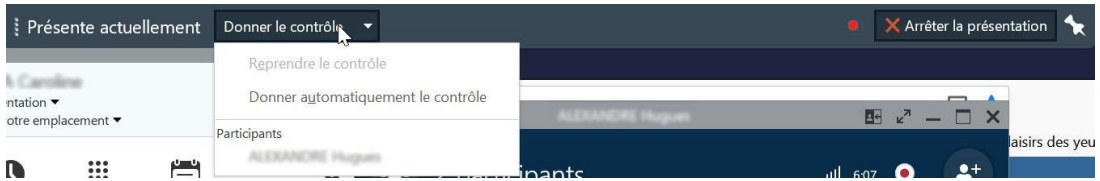
1. Demande à l'usager de partager son écran
2. Demande de prise de contrôle par le SI



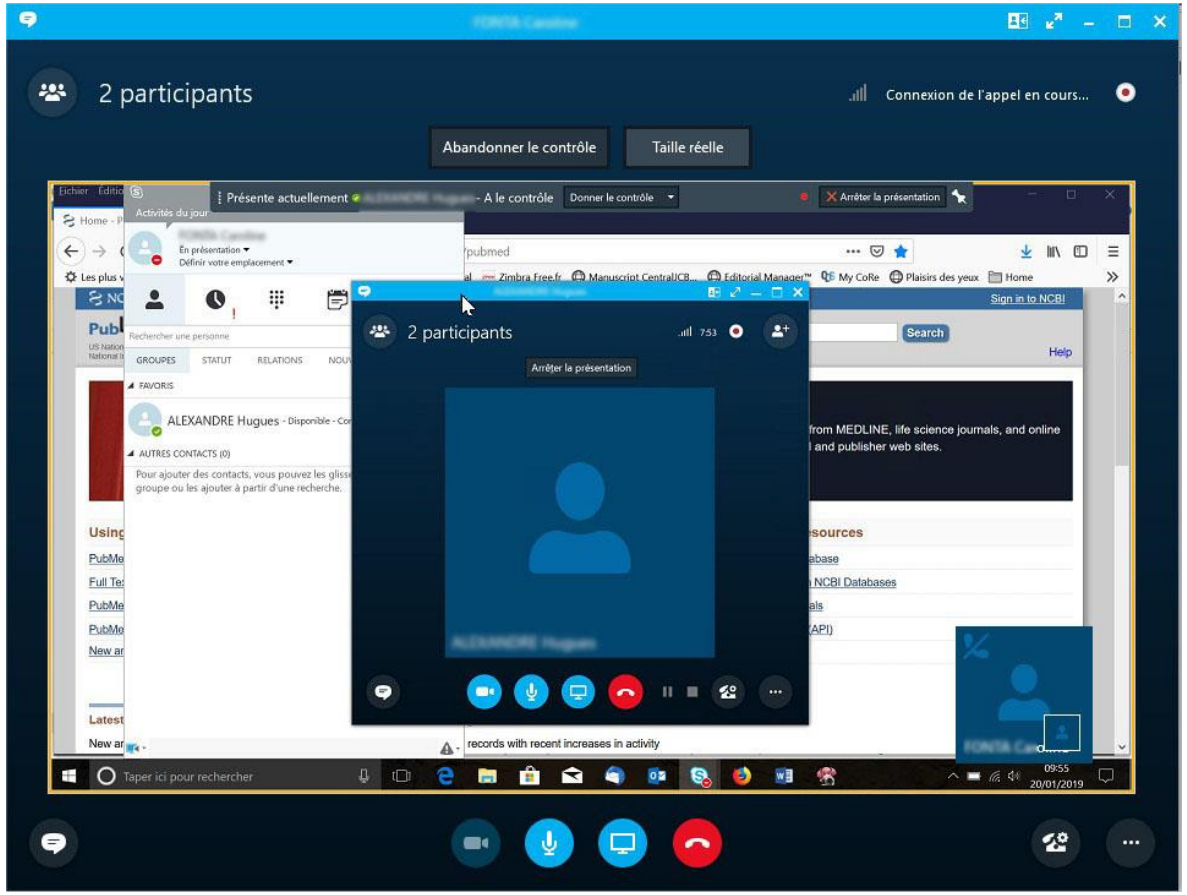
Assistance distante

1

2

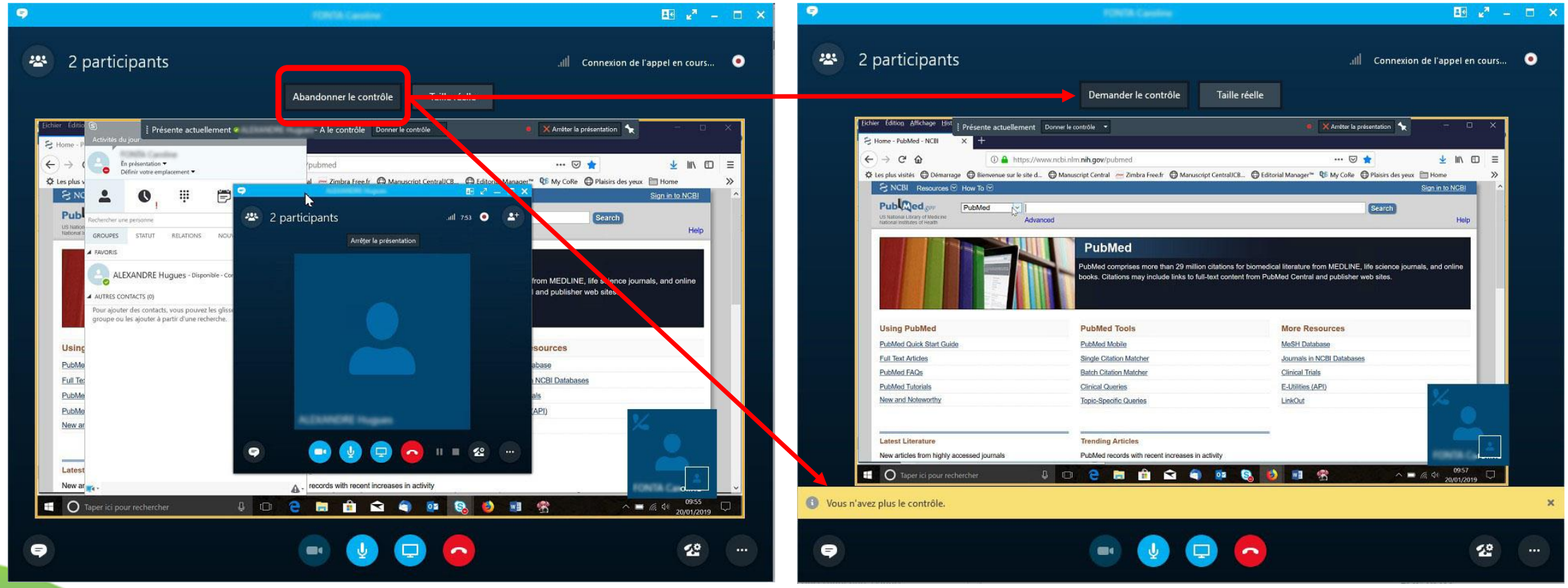


3



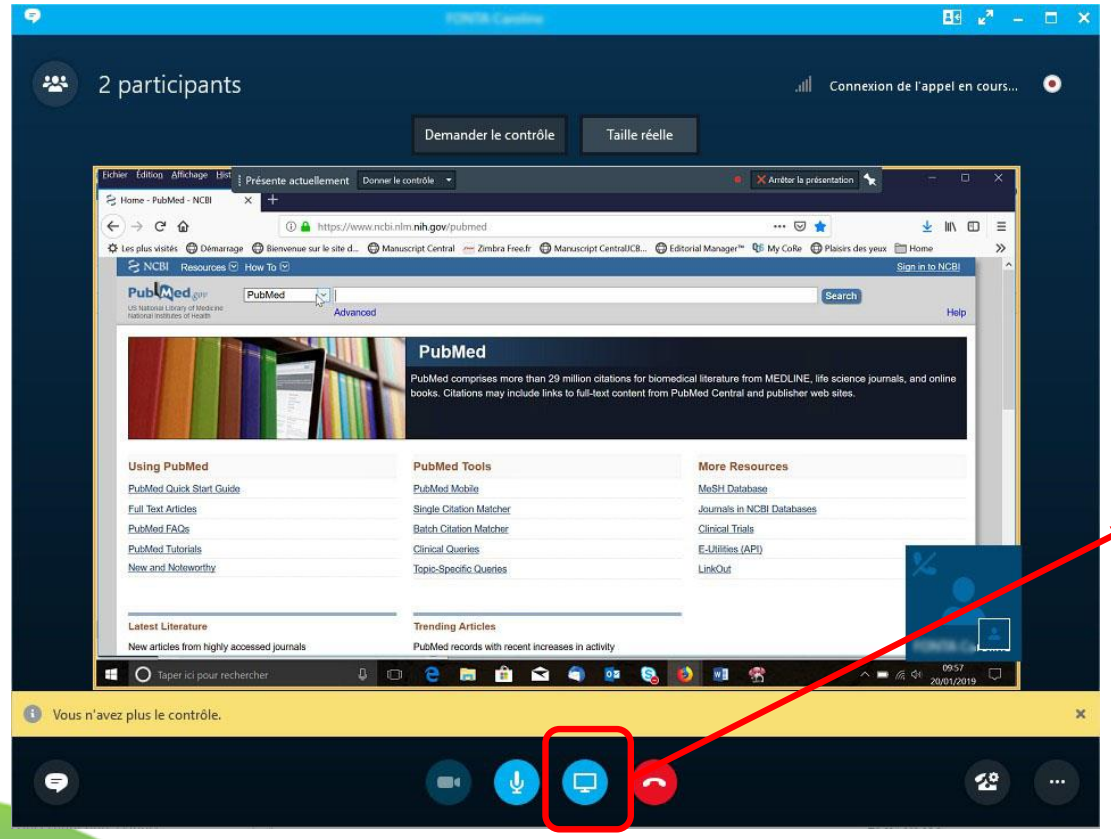
EcoLab

Assistance distante

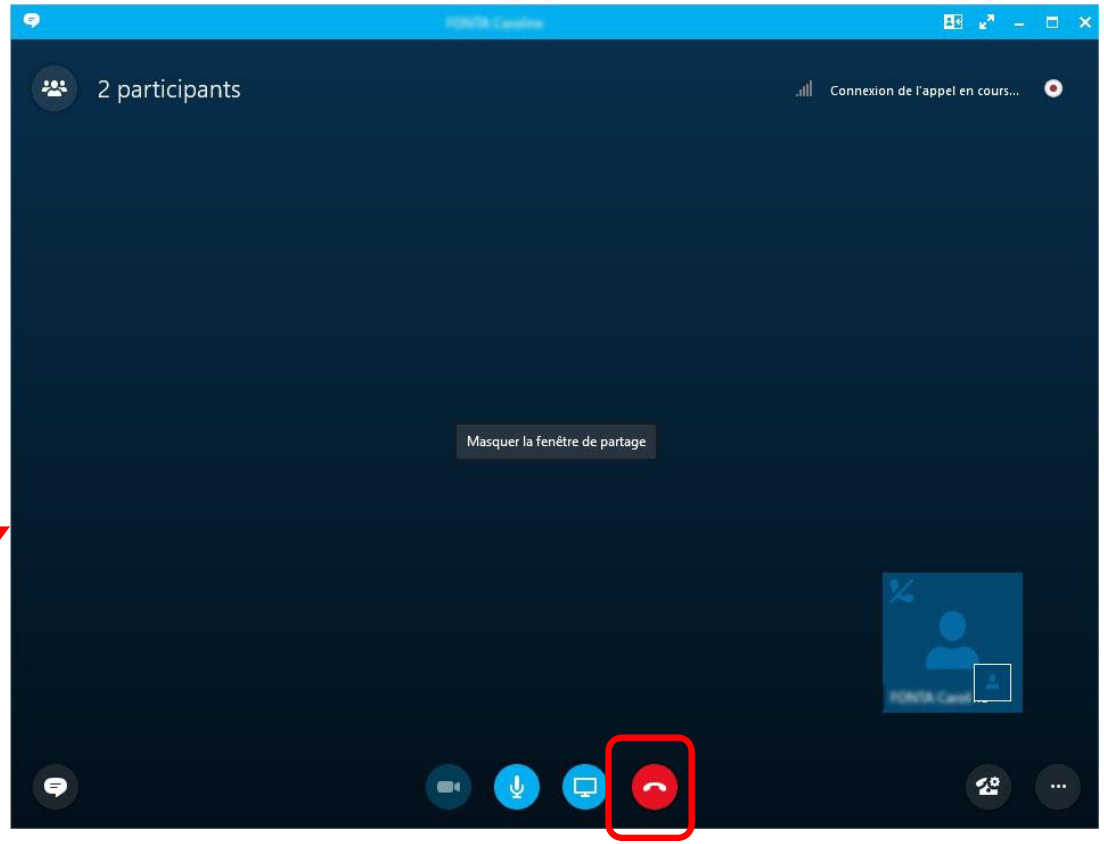


EcoLab

Assistance distante



Arrêt du partage



Fin de communication et assistance

EcoLab

Merci pour votre attention

Une démo ?

Des questions ?

☺