Donner les droits de création de VMs à un groupe d'utilisateurs

Documentation VMware : Privilèges requis pour les tâches courantes (Créer une machine virtuelle)
http://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.security.doc/GUID-4D0F8E63-2961-4B71-B365-BBFA24673FDB.html#GUID-4D0F8E63-2961-4B71-B365-BBFA24673FDB

Présentation

- Permettre à un groupe d'utilisateurs de pouvoir créer et gérer leurs VMs
- Sans disposer de droits supplémentaires sur le serveur

Principes

- Créer un **dossier** spécifique dans le **centre de données** ;
- Créer un **groupe de ressources** spécifique sur un **hôte physique** ;
- ce groupe de ressources précise éventuellement les limitations des ressources à utiliser (Ressources CPU et Mémoire RAM) ;
- les utilisateurs sont **administrateur** de ce groupe de ressources ;
- il est nécessaire de permettre :
  - de pouvoir créer une VM dans le centre de données ;
  - d'allouer de l'espace disque dans la banque de données ;
  - de parcourir la banque de données pour associer un fichier iso au lecteur de CD-ROM de la VM
  - de pouvoir assigner un réseau à la VM (parmi les VLANs disponibles)
- Pour cela et pour faire simple, un seul rôle appelé **Créateur VMs** est créé et regroupe ces privilèges particuliers.

Résumé des privilèges requis :

Privilège	**Objet concerné**	**Rôle attribué**
Machine virtuelle.Inventaire .Créer	Pool de ressources concerné	Administrateur
	Dossier spécifique	Créateur VMs
Machine virtuelle.Configuration.Ajouter un nouveau disque (en cas de création d'un nouveau disque virtuel)	Pool de ressources concerné	Administrateur
Machine virtuelle.Configuration.Ajouter un disque existant (en cas d'utilisation d'un disque virtuel existant)	Pool de ressources concerné	Administrateur
Ressource.Attribuer une machine virtuelle au pool de ressources	Pool de ressources concerné	Administrateur
Banque de données.Allouer de l'espace	Dossier spécifique	Créateur VMs
Banque de données.Parcourir banque de données	Dossier spécifique	Créateur VMs
Réseau.Assigner un réseau	Réseau concerné	Créateur VMs

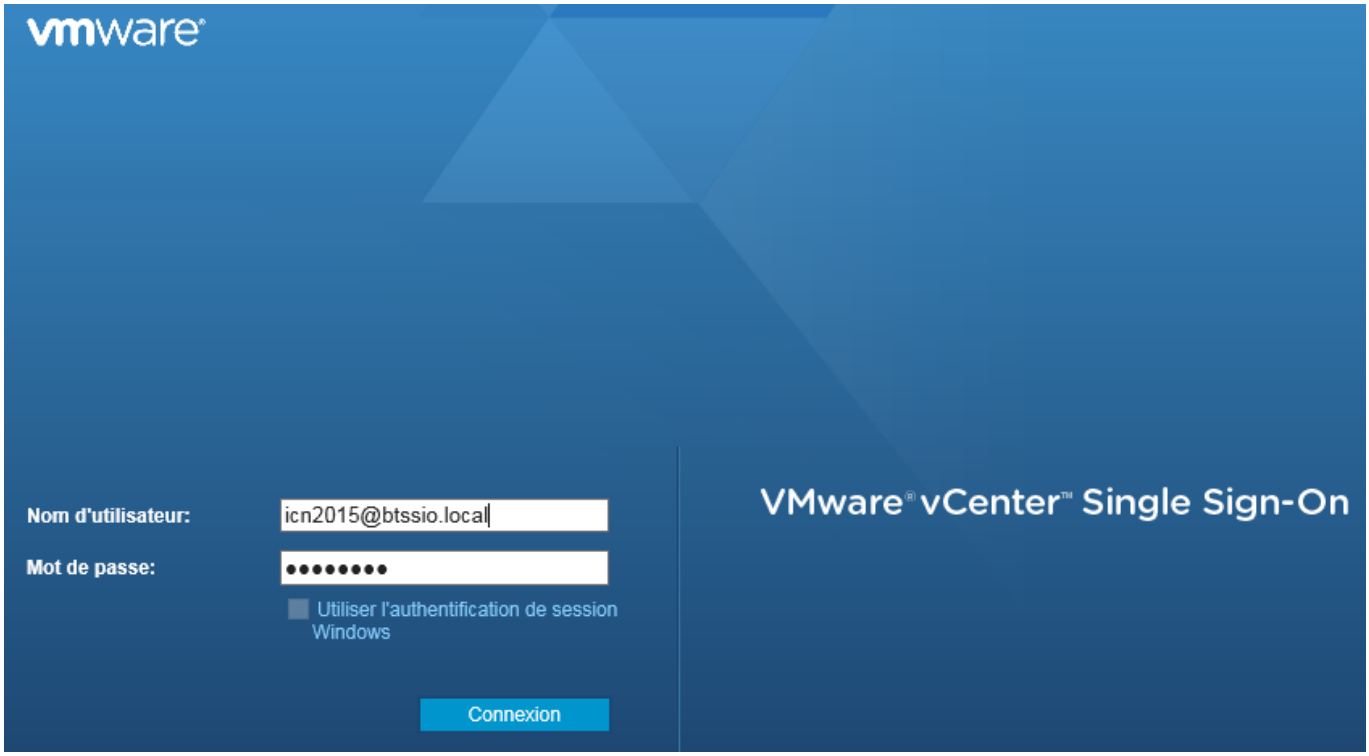
Mise en oeuvre

La mise en oeuvre de cette gestion se fera, à titre d'exemple, avec les informations suivantes :

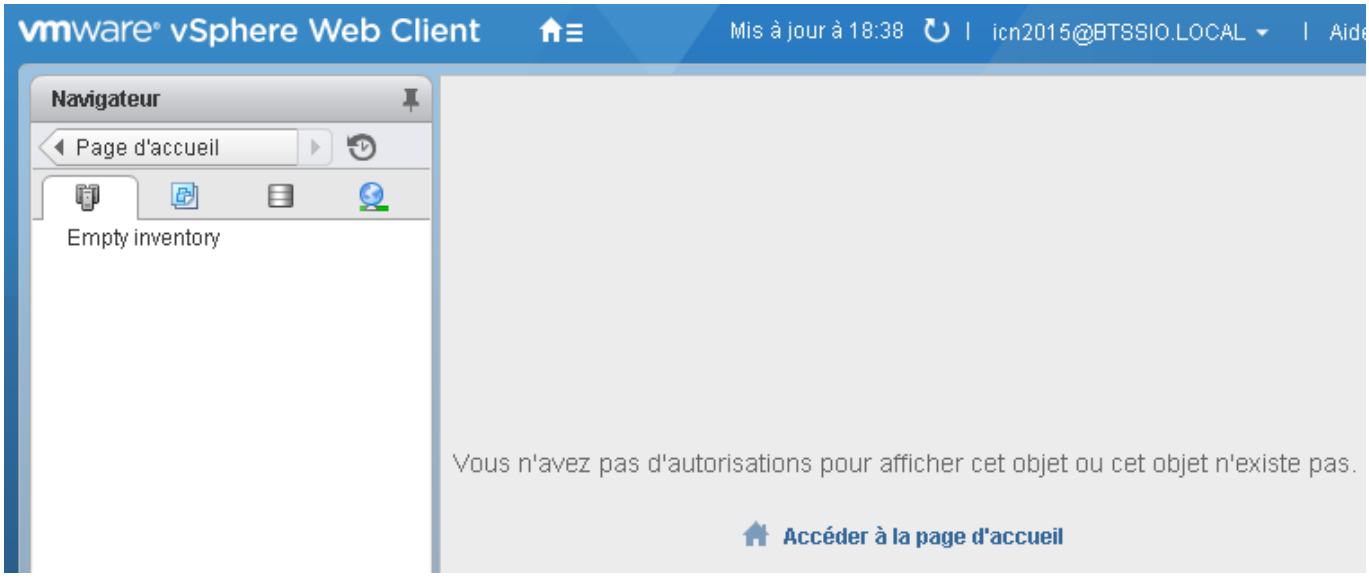
- **Compte utilisateur** utilisé dans le domaine BTSSIO.LOCAL : icn2015
- Ce compte appartient au **groupe utilisateur** : G_Valadon_2015_ICN
- Création d'un **dossier ICN** dans le **centre de données**
- Création du rôle **Createur VMs**

Ouverture de session de l'utilisateur

- compte **icn2015** du domaine **BTSSIO.LOCAL**

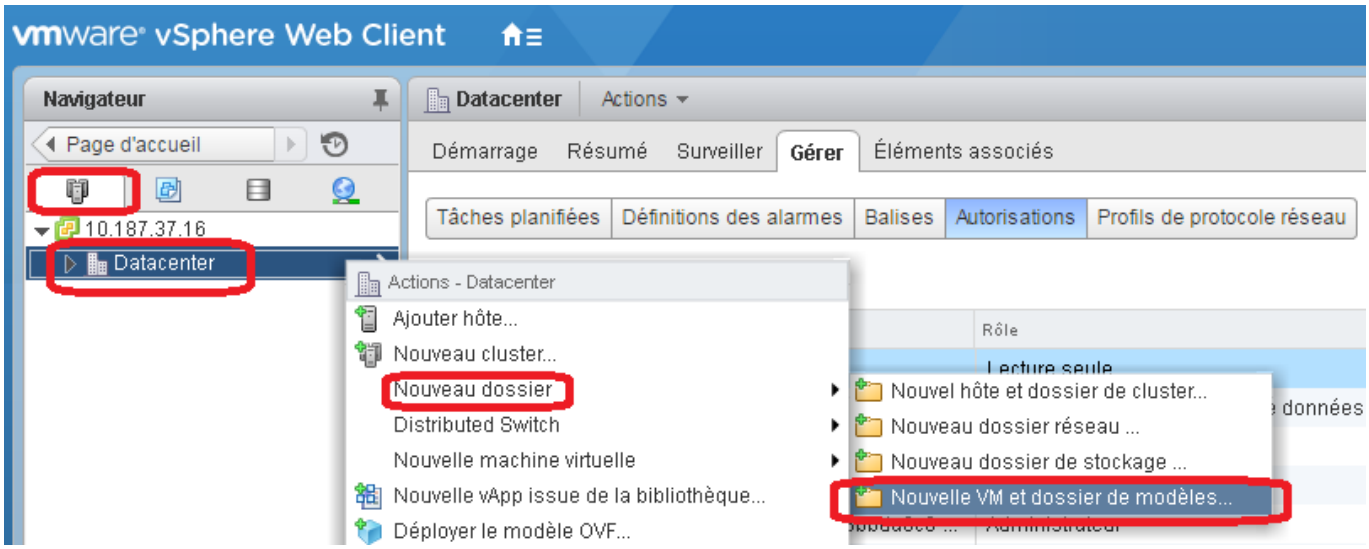


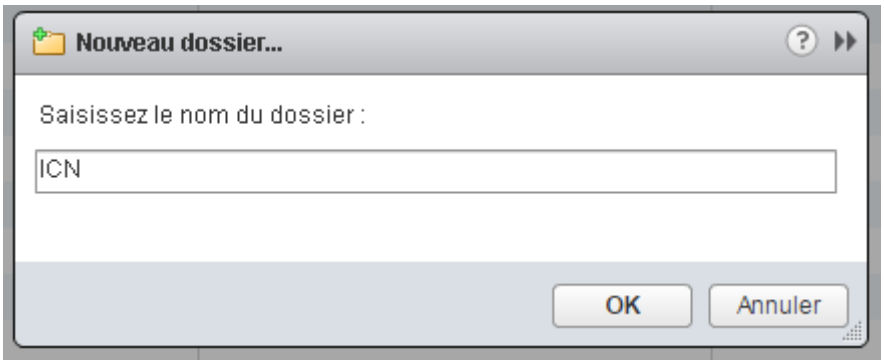
- n'ayant aucune autorisation, ce compte ne peut accéder aux ressources



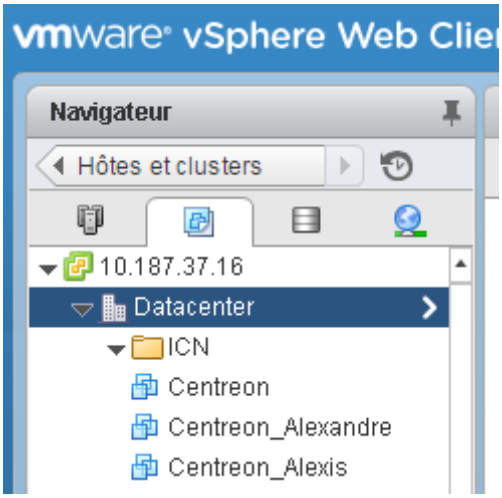
Création du dossier ICN

Au niveau des **hôtes et Clusters**, création du **dossier ICN** dans le **centre de données** existant **Datacenter** :





Au niveau **VM et modèles** on visualise le dossier ICN créé :



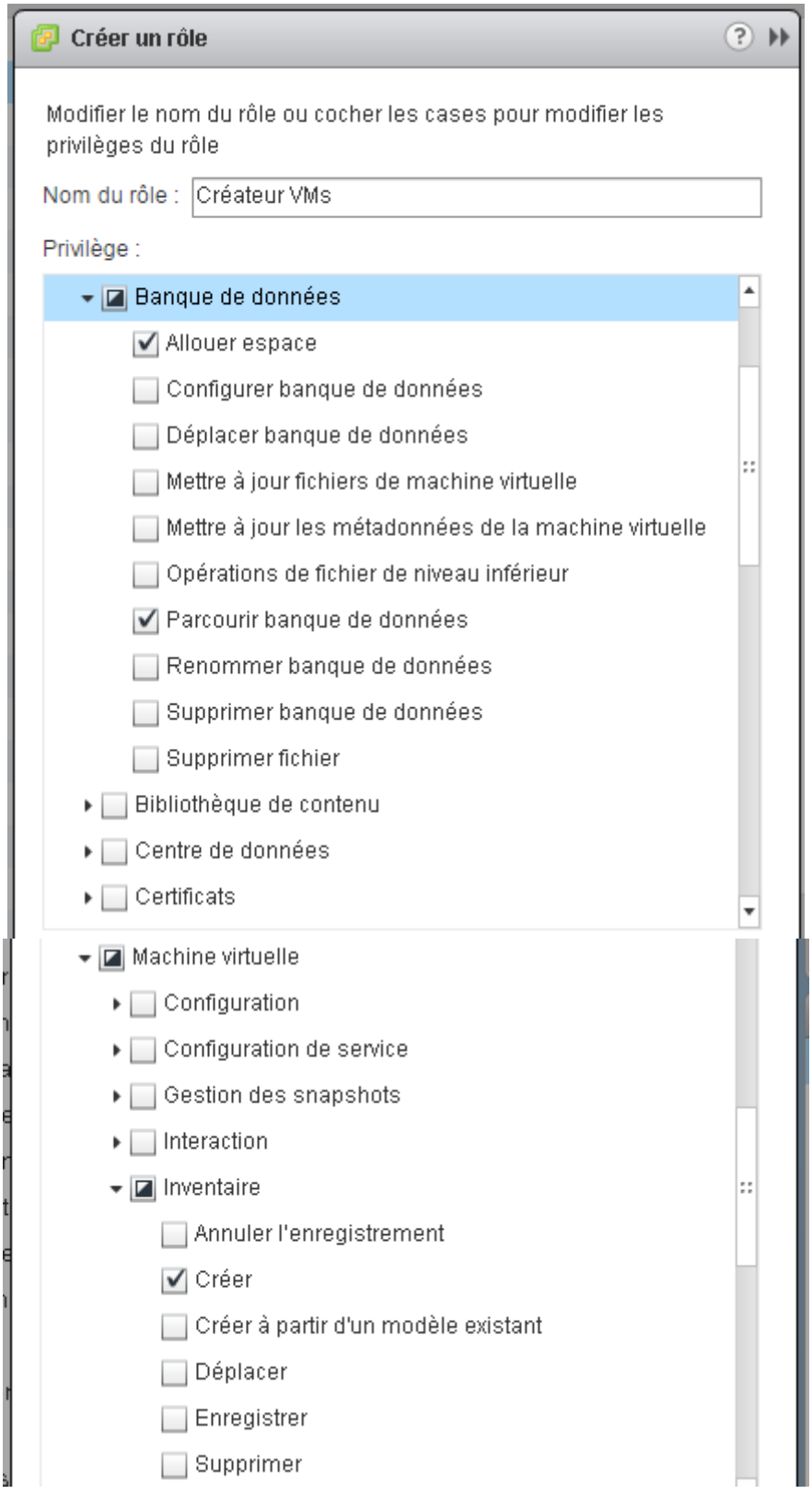
Création d'un rôle

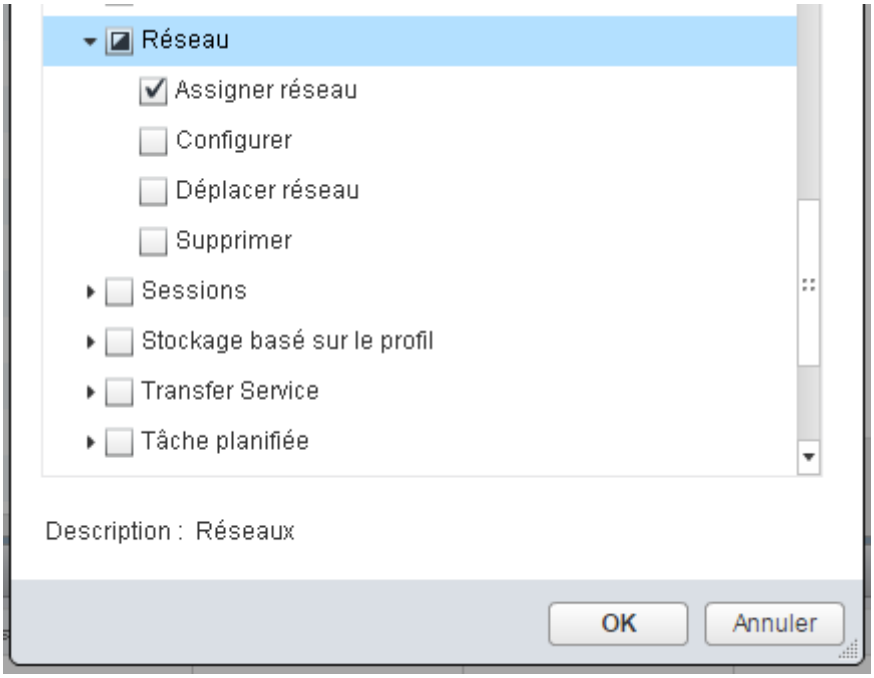
Pour faire simple, un seul rôle supplémentaire appelé **Créateur VMs** est créé avec les privilèges nécessaires. Ce rôle sera utilisé sur plusieurs objets, là où cela est requis.

Privilèges associés à ce rôle

- Banque de données.Allouer de l'espace
- Banque de données.Parcourir banque de données
- Machine virtuelle.Inventaire .Créer
- Réseau.Assigner un réseau

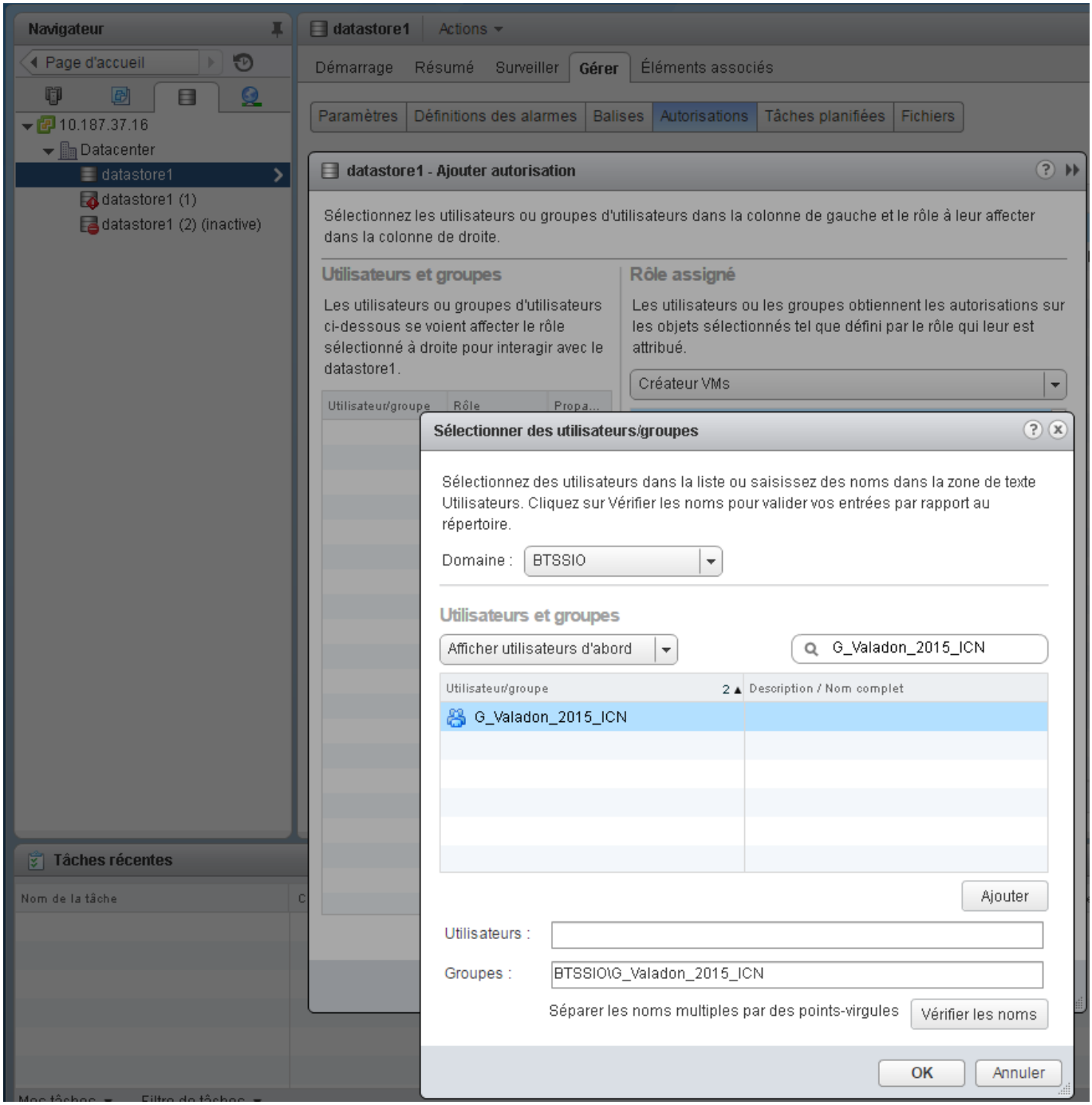
Création du rôle et définition des privilèges

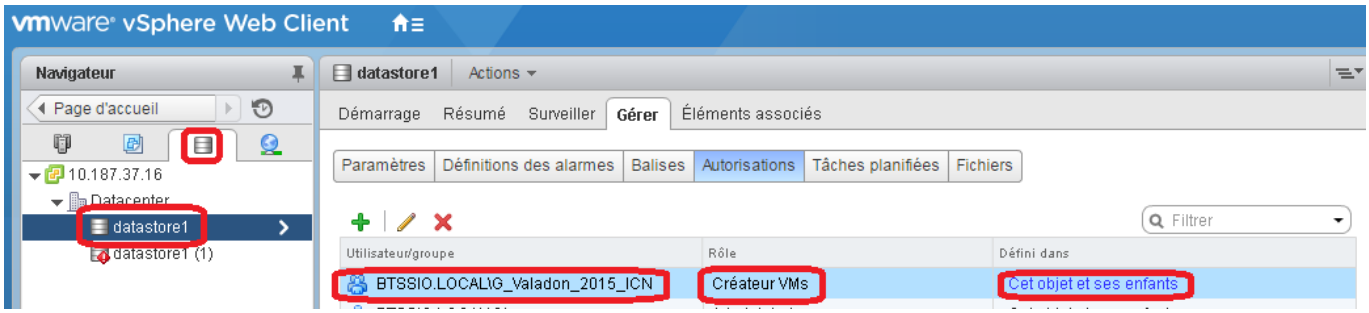

Créer un rôle
Modifier le nom du rôle ou cocher les cases pour modifier les privilèges du rôle
Nom du rôle : Créateur VMs
Privilège :
Banque de données
Allouer espace
Configurer banque de données
Déplacer banque de données
Mettre à jour fichiers de machine virtuelle
Mettre à jour les métadonnées de la machine virtuelle
Opérations de fichier de niveau inférieur
Parcourir banque de données
Renommer banque de données
Supprimer banque de données
Supprimer fichier
Bibliothèque de contenu
Centre de données
Certificats
Machine virtuelle
Configuration
Configuration de service
Gestion des snapshots
Interaction
Inventaire
Annuler l'enregistrement
Créer
Créer à partir d'un modèle existant
Déplacer
Enregistrer
Supprimer



Donner l'autorisation d'écrire et de parcourir la banque de données en utilisant le rôle Créateur VMs

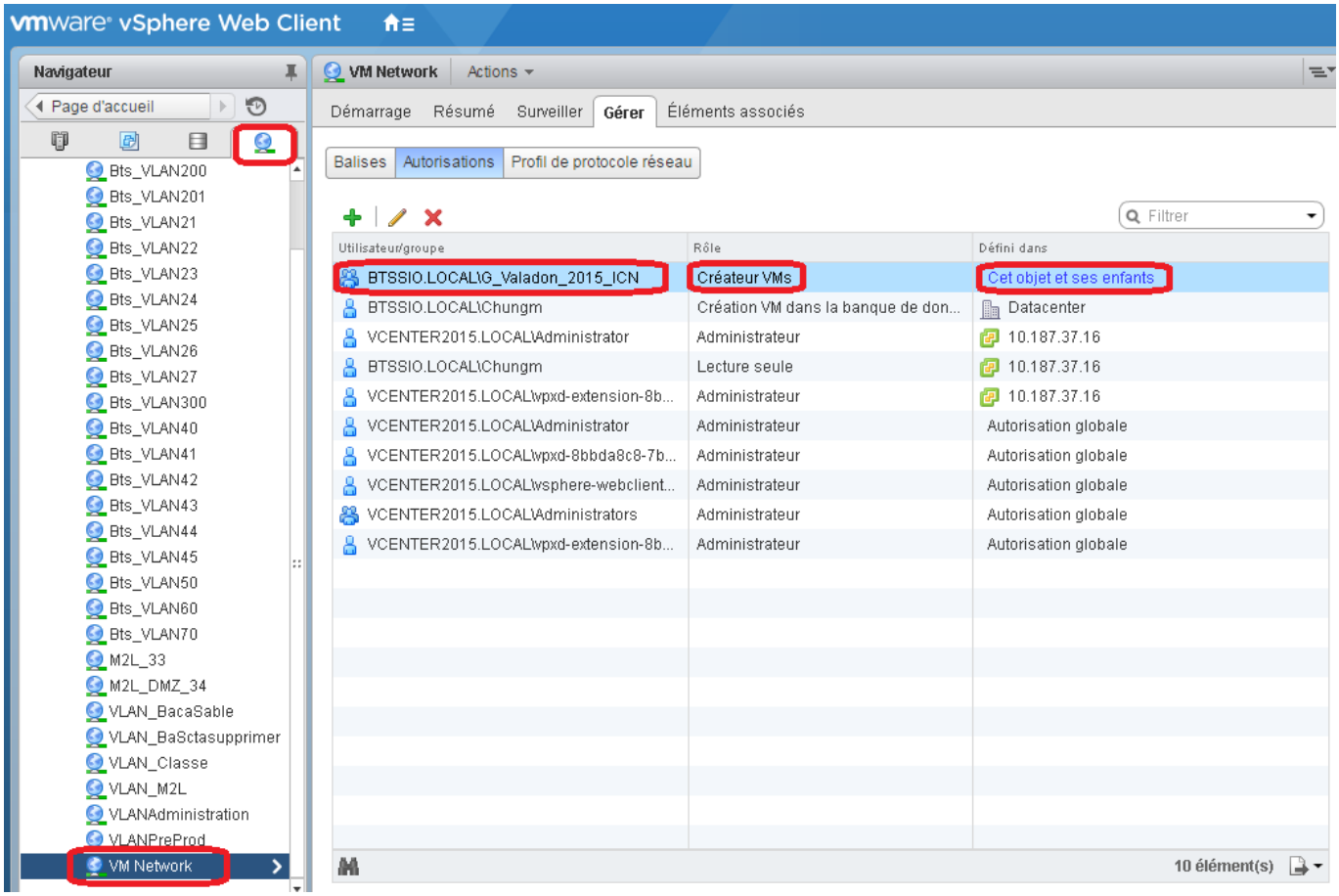
Cette autorisation est uniquement définie pour la banque de données de l'un des ESX qui est appelée **datastore1** dans Vsphère.





Donner l'autorisation d'assigner un réseau précis aux VMs créées

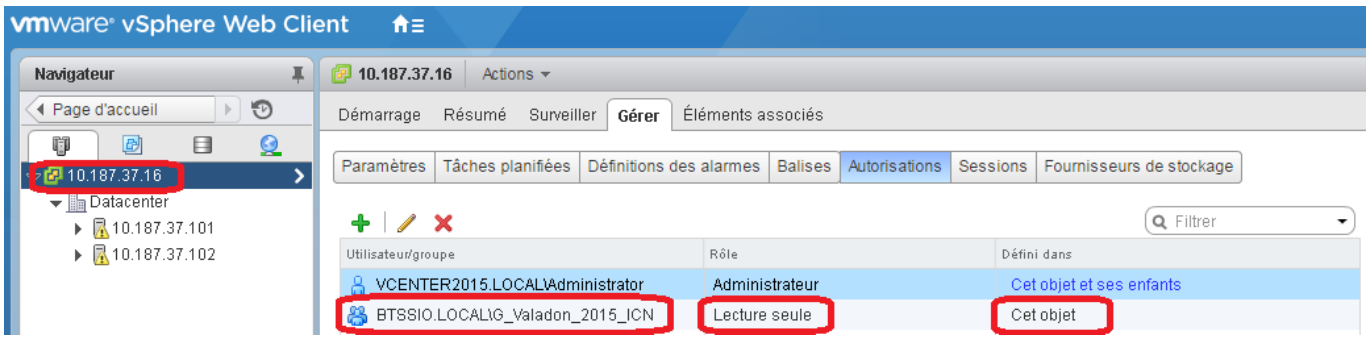
Cette autorisation est uniquement définie pour le réseau VM Network. Il est bien sûr possible, comme pour les autorisations précédentes, de le faire à un niveau supérieur pour permettre l'utilisation de tous les réseaux (VLANs)



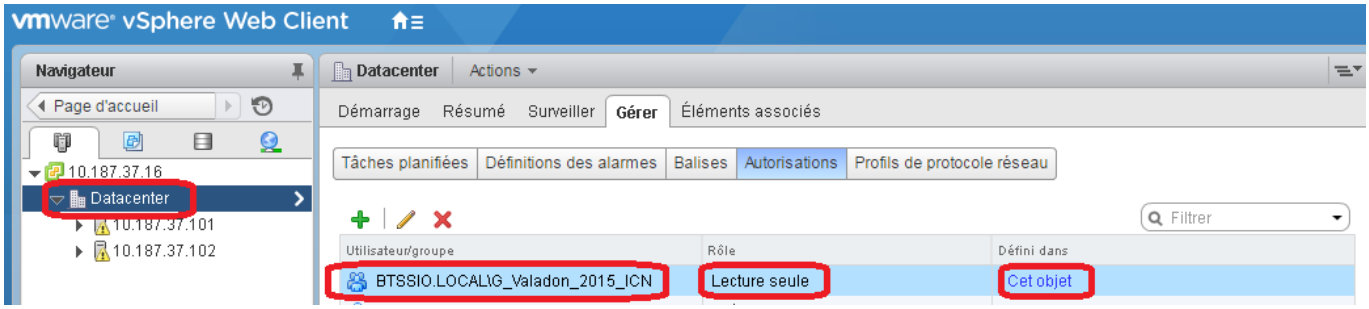
Affecter les bonnes autorisations pour limiter ce que peut faire l'utilisateur

Attention : pour gérer ce que **peut** ou ne peut pas **voir** et **faire** l'utilisateur, il faudra cocher ou pas l'option **Propager vers les enfants**, c'est à dire limiter ou pas le rôle à l'objet.

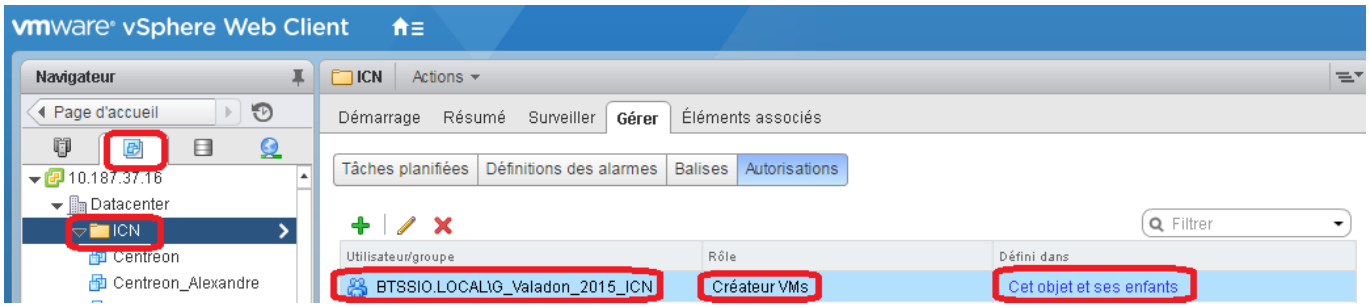
Attribuer le rôle lecture seule uniquement sur l'objet Vsphère



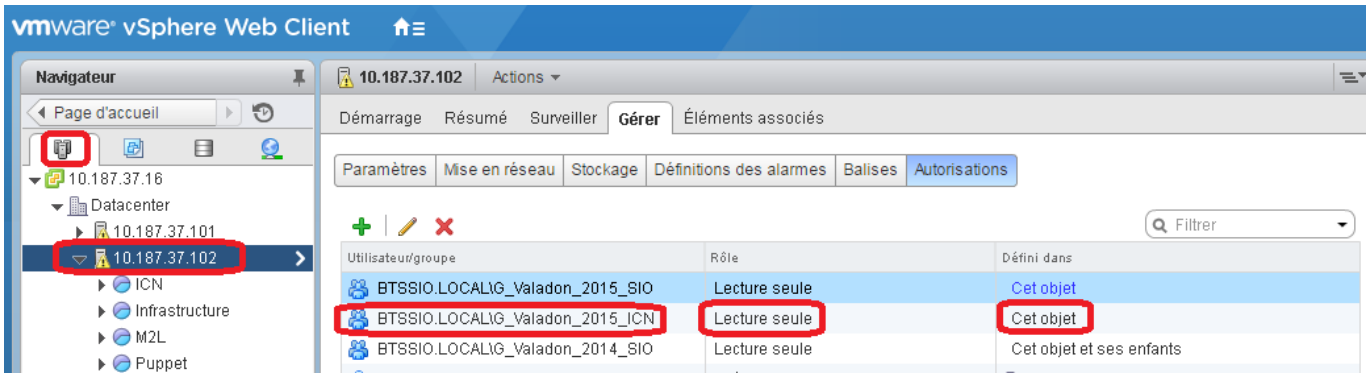
Attribuer le rôle lecture seule uniquement sur le centre de données



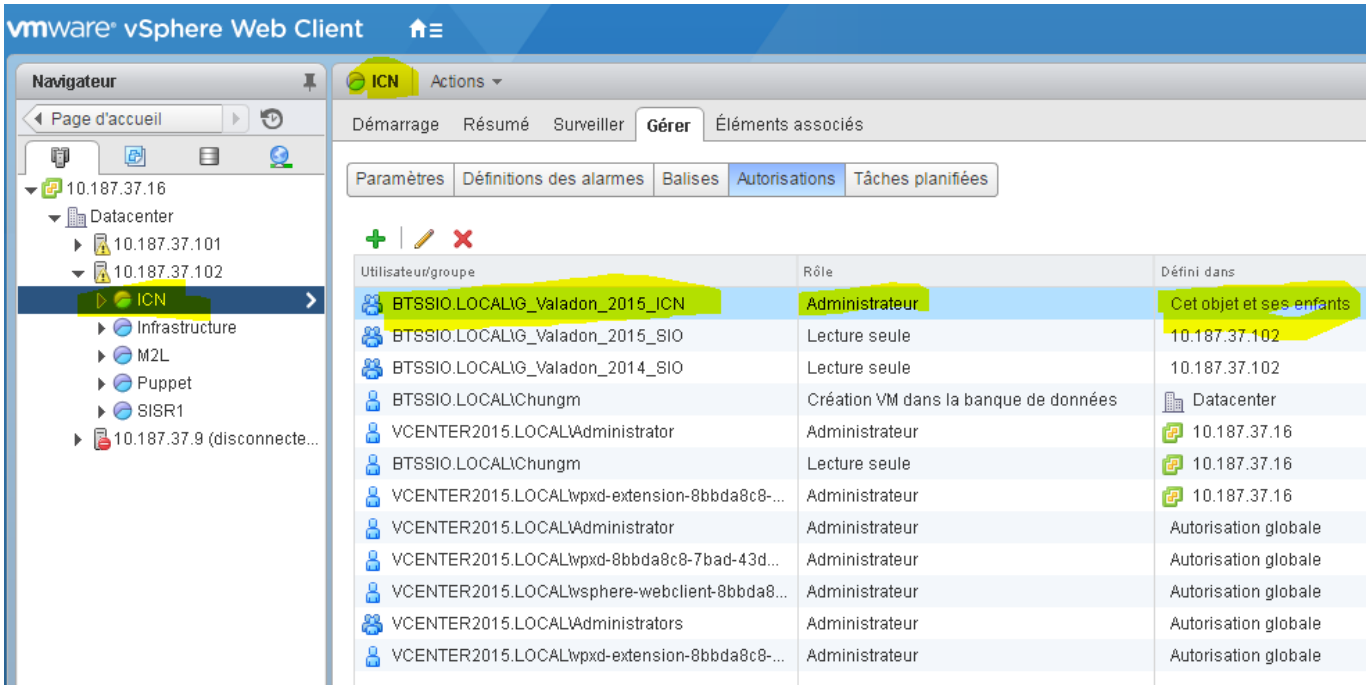
Attribuer le rôle Créateur VMs sur le dossier ICN



Attribuer le rôle lecture seule uniquement sur l'hôte physique

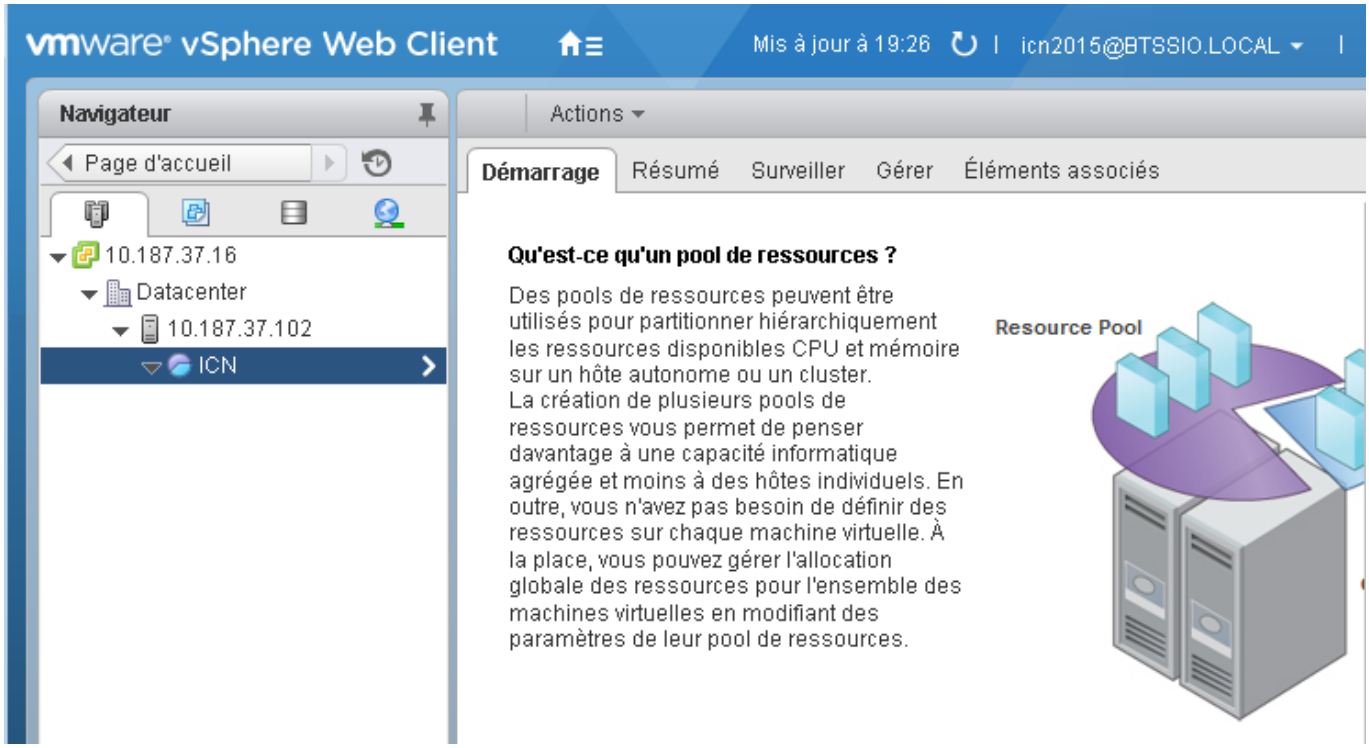


Attribuer le rôle Administrateur sur le pool de ressources ICN



Création d'une VM par l'utilisateur icn2015

En rafraîchissant l'affichage, ou en se reconnectant, l'utilisateur accède au pool de ressources et peut créer sa VM.



Lors de la création, développez l'arborescence pour choisir le dossier ICN :