



IBM Power Systems - IBM i

Modernisation, développement d'applications et DB2 sous IBM i
Technologies, outils et nouveautés 2013-2014

13 et 14 mai 2014 – IBM Client Center Paris, Bois-Colombes

**S28 - La mise en œuvre de SSO (*Single Sign On*) avec EIM
(*Enterprise Identity Mapping*)**

Mercredi 14 mai – 15h15-16h45

Dominique GAYTE – NoToS – dgayte@notos.fr



NoToS

- Expertise autour de l'IBM i
 - 25 ans d'expérience sur AS/400
 - Regard moderne
- PHP sur IBM i avec Zend
- Développement de progiciels
 - PHP

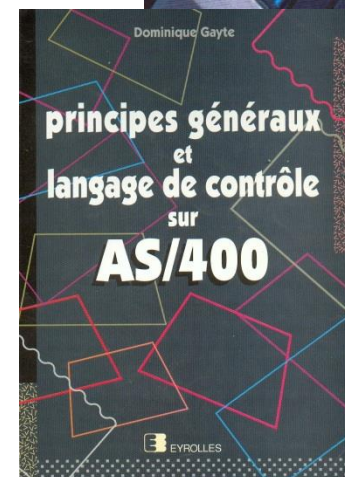


Valorisation des spools des IBM i (AS/400)
Transformation en PDF, archivage, indexation
<http://www.notos.fr/phpSpool.aspx>



Gestion de Contenu (ECM)
GED, graphiques, alertes, workflow, GANTT...
<http://www.lorena.pro>

- Service
 - Formation, audit, développement...



Sommaire

- Pourquoi un SSO ?
- Le service d'authentification réseau (NAS)
- EIM
- Les mappages
- Les pièges à éviter

Pourquoi un SSO ?

- Les identifiants/mots de passe sont les protections essentielles de nos systèmes d'information
- Identifiants pour les applications locales
 - Windows
 - Messagerie (Exchange, Domino/Lotus Notes...)
 - Différents IBM i
 - Serveurs Web
 - ...

Pourquoi un SSO ? (2)

- Une surcharge de travail pour les administrateurs
 - Gestion de plusieurs solutions et plates-formes d'authentification :
1 utilisateur = n comptes, n userID, n mots de passe
 - 30% (de 20 à 40) des appels vers le Help Desk de l'entreprise concernent directement des problèmes d'accès rencontrés par les utilisateurs lors de leur authentification
 - D'où une simplification des processus de connexions utilisateurs pouvant induire des failles de sécurité

- Pour les utilisateurs
 - Saisie au quotidien de plusieurs identifiants et mots de passe pour accéder aux données et applications de l'entreprise
 - Gestion de multiples identifiants / mots de passe et des règles associées
 - Attention aux transgressions des règles de sécurité

Définition

- SSO : « *Single Sign-On* »
- Système de signature unique
- Solution qui permet aux utilisateurs d'un réseau d'entreprise d'accéder à l'ensemble des ressources autorisées, sur la base d'une authentification unique effectuée lors de l'accès initial au réseau
- Objectifs
 - Simplifier les procédures d'authentification des utilisateurs
 - Renforcer le niveau de sécurité du système d'information
 - Rationaliser la gestion des comptes

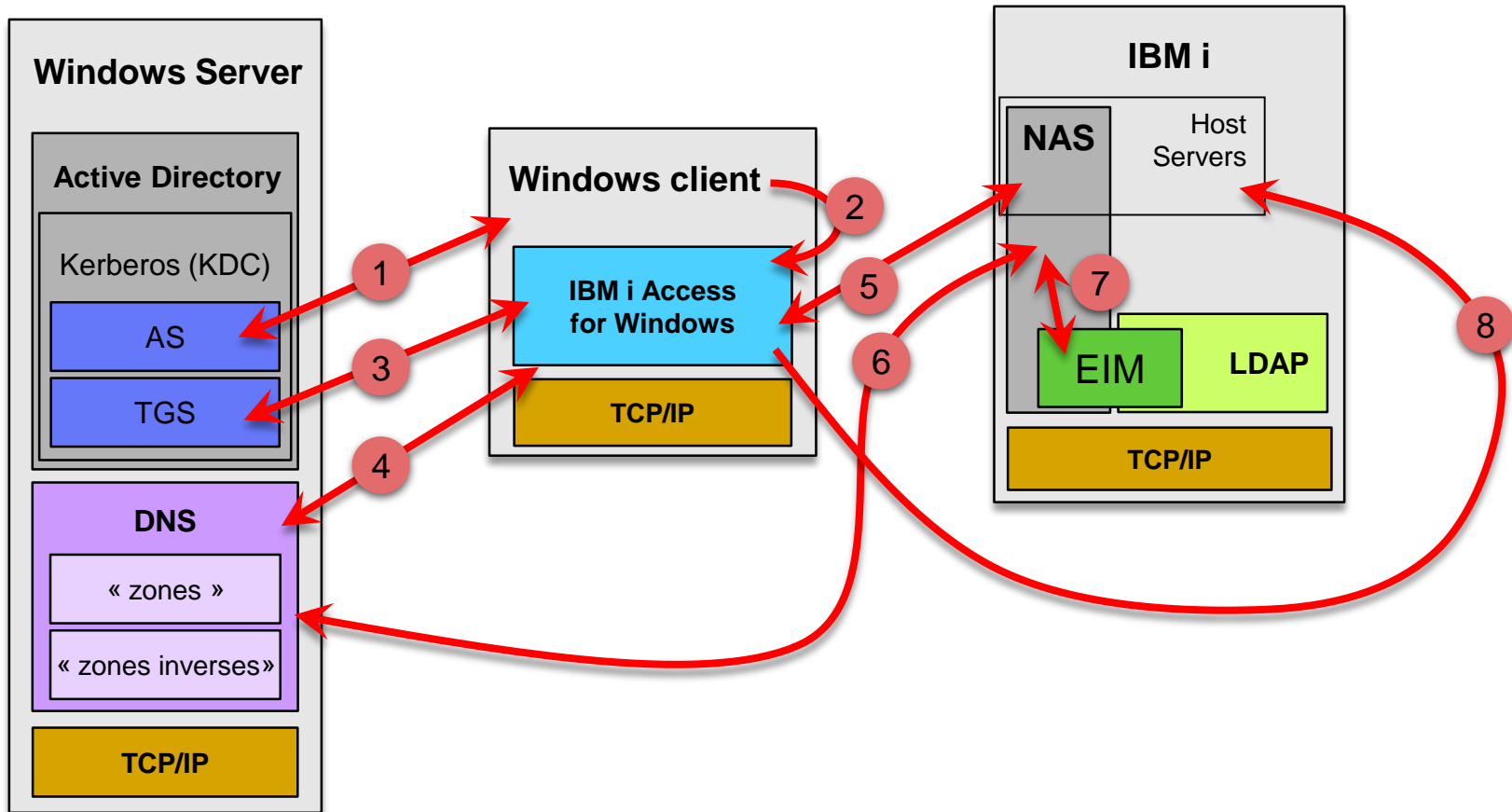
Authentification et Autorisation

- Authentification
 - Décliner son identité et prouver que l'on est bien celui que l'on prétend être
- Autorisations
 - Vérifier que la personne authentifiée a bien les autorisations nécessaires pour réaliser ce qu'elle demande
- Une solution de SSO doit prendre en compte authentification et autorisations

SSO sur IBM i

- Le SSO s'appuie sur 2 technologies
 - Authentification avec Kerberos (*Network Authentication Service*)
 - Autorisation avec EIM (*Enterprise Identity Mapping*)
- Le SSO n'est disponible que si c'est deux technologies sont bien configurées et mises en œuvre
- L'IBM i fait confiance à l'authentification réalisée par Kerberos
 - Le plus souvent, il s'agit d'un Active Directory
 - Lors de l'ouverture de la session Windows

SSO/EIM : schéma général avec un AD



SSO EIM et IBM i : que faut il ?

- Un serveur Kerberos
 - Windows 2xxx avec Active Directory
 - Ou un serveur Unix/Linux avec Kerberos Server
 - ou System i V5R3 avec Kerberos Server
 - c'est le serveur AIX, sous PASE
- Sur l'IBM i participant (V5R2 minimum)
 - 5722-SS1 Option 12 OS/400 - Serveurs hôte
 - 5722-SS1 Option 30 OS/400 - Qshell
 - 5722-AC3 Crypto Access Provider 128-bit (pour serveur Kerberos)
 - sauf > V5R4 : Network Authentication Enablement (5722-NAE)
- Sur le client
 - Microsoft Windows XP/2000/2003/7/8...
 - IBM i Access for Windows (V5R2 minimum)

Le service d'authentification réseau (NAS)

- Kerberos est un protocole d'authentification réseau créé par le MIT qui utilise une cryptographie à clés symétriques pour authentifier les utilisateurs auprès de services réseau, éliminant par la même la nécessité de transmettre des mots de passe sur le réseau
- Pas de transmission de mot de passe
 - L'IBM i ne recevra jamais le mot de passe Windows !
 - Juste un ticket (crypté et horodaté) lui indiquant que l'utilisateur a bien été authentifié par l'AD
 - L'IBM i fera confiance à cette authentification



Le service d'authentification réseau (NAS) (2)

- Les profils utilisateur participant à EIM peuvent ne plus avoir de mot de passe (PASSWORD(*NONE))
- MAIS...
 - Kerberos ne fournit pas d'autorisations uniquement de l'authentification
 - C'est EIM qui en sera chargé
 - Kerberos ne fait pas de chiffrement de données
 - C'est SSL qui le fait si besoin

Comment faire ?

- Configuration du réseau
 - DNS & Reverse DNS
- Configuration du NAS sur l'(es) IBM i
- Configuration de l'AD
 - Création des quelques comptes
 - Scripts générés automatiquement
- Tests de la couche Kerberos (NAS)
- Configuration EIM dans l'(es) IBM i
 - Création des associations Compte AD => Profil utilisateur
- Test des applications sur le poste de travail

Configuration du réseau

- Kerberos est très sensible à la configuration du réseau. Il faut une parfaite cohérence entre :
 - Les noms sous lesquels les systèmes se connaissent
 - Les noms résolus par les DNS
 - Les adresses IP résolues par les Reverse DNS
- Les IBM i ne sont pas toujours bien définis dans TCP/IP
 - Héritages de SNA...
 - Ils ont souvent plusieurs noms
- Ils ne sont pas toujours bien configurés dans les DNS
- Le Reverse DNS parfois n'existe pas
- Attention aux décalages d'horloges

Configuration du NAS sur l'IBM i

- Vérification de la configuration IP
- CFGTCP option 12
 - Nom
 - Domaine
 - Priorité de recherche à *LOCAL
 - DNS
- CFGTCP option 10
 - Nom long en premier

```

Change TCP/IP Domain (CHGTCPDMN)

Indiquez vos choix, puis appuyez sur ENTREE.

Host name . . . . . 'MANTE'
Domain name . . . . . 'NOTOS.BEAULIEU'

Domain search list . . . . . *DEF

Host name search priority . . . *LOCAL *REMOTE, *LOCAL, *SAME

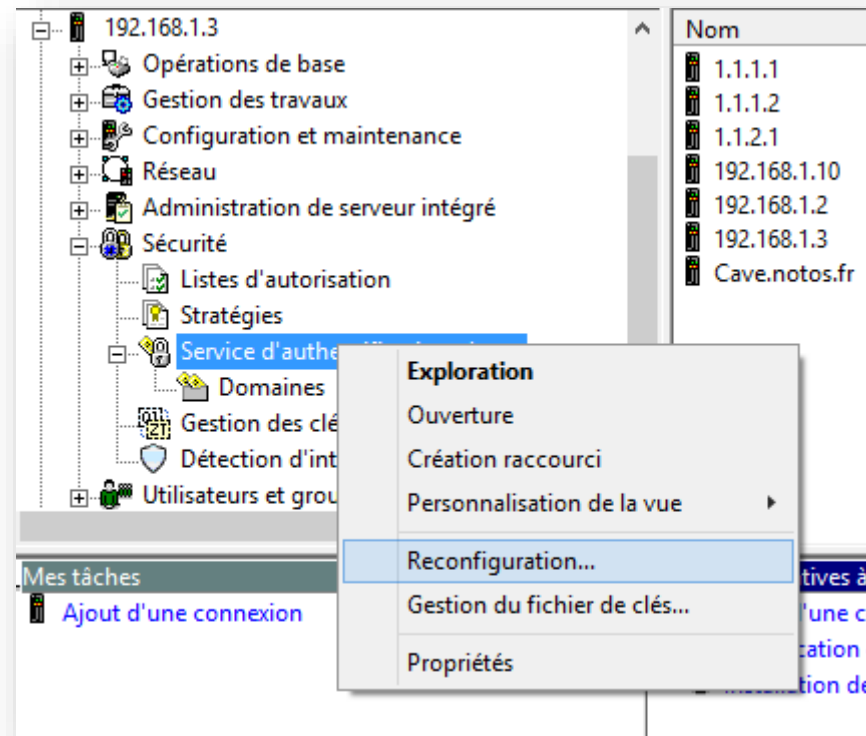
Domain name server:
  Internet address . . . . . '192.168.1.110'
  Internet address . . . . . '192.168.1.254'
  Internet address . . . . . *SAME
  
```

```

_ 127.0.0.1 LOOPBACK
LOCALHOST
_ 192.168.1.3 MANTE.NOTOS.BEAULIEU
MANTE
  
```


Assistant de configuration d'IBM i Navigator

- Configuration ou Reconfiguration



Configuration du service d'authentification réseau



Pour utiliser kerberos, un système doit être configuré comme faisant partie d'au moins un domaine kerberos. Ce domaine est considéré comme le domaine par défaut pour le système.

Quel est le domaine kerberos par défaut à associer à ce système ?

Domaine par défaut : NOTOS.BEAULIEU

Microsoft Active Directory



Un centre KDC (Centre de distribution de clés) kerberos a deux fonctions. Il authentifie les principaux dans le domaine et fournit des tickets d'autorisation que les clients utilisent pour s'authentifier auprès des services kerberos activés.

Quel nom souhaitez-vous donner au centre KDC associé au domaine par défaut ?

Centre KDC : 192.168.1.110

Port : 88



Le serveur de mots de passe kerberos permet aux clients de modifier à distance leur mot de passe d'accès au centre KDC. En général, ce serveur s'exécute sur la même machine que le centre KDC.

Souhaitez-vous configurer ce système afin qu'il utilise un domaine par défaut ?

Oui

Serveur de mots de passe : 192.168.1.110

Port : 464

Non

< Précédent Suivant >



Les services kerberos activés nécessitent un fichier de clés pour l'authentification des identités client. Ce type de fichier permet de stocker en toute sécurité une version chiffrée des clés à long terme du nom principal de service.

Choisissez le ou les services pour lesquels vous souhaitez ajouter ou mettre à jour un poste dans le fichier de clés.

- Authentification kerberos i5/OS
- LDAP
- Serveur HTTP optimisé par Apache
- i5/OS NetServer
- Serveur NFS System i


Cliquez sur le bouton Détails afin d'afficher la liste des postes de fichier de clés qui existent déjà sur le serveur et qui sont manquants.

Détails...

< Précédent Suivant > Terminer Annuler

Erreur potentielle !

- Le poste local (PC) et l'IBM i ne font pas la même résolution



L'authentification kerberos utilise des noms d'hôte lors de la création de tickets d'autorisation pour les clients. Pour cette raison, il est important que les noms d'hôte résolus par les clients et les serveurs du réseau soient identiques. Actuellement, le nom d'hôte résolu par i5/OS à partir du serveur i5/OS cible ne correspond pas au nom d'hôte client résolu à partir de votre machine sur laquelle s'exécute IBM System i Access for Windows.

Nom hôte résolu par le client :

Nom hôte résolu par i5/OS :

Les postes de fichier de clés supplémentaires pour le nom d'hôte résolu par le serveur i5/OS cible vont être ajoutés pour tous les types de fichiers de clés déjà existants dans le fichier de clés ainsi que ceux qui ont peut-être été sélectionnés précédemment dans cet assistant.

Remarque : Ces modifications concernent uniquement les entrées du fichier de clés. Cependant, l'administrateur du centre de distribution de clés (KDC) devra créer des noms principaux de service kerberos pour les deux noms d'hôte résolus dans le centre KDC.

Cliquez sur le bouton Détails pour plus d'informations sur la résolution des conflits de noms d'hôte.

Détails...

< Précédent Suivant > Terminer Annuler

Création des postes de fichier de clés

- Fichier de clés
 - /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab
- Krbsrv400 : pour tout ce qui est IBM i Access



Certaines fonctions permettant l'ouverture de session unique, dont IBM System i Access for Windows, font un grand usage des noms principaux de service kerberos ci-après pour l'authentification des clients. Ces postes de fichiers de clés sont utilisés pour l'authentification kerberos de sorte qu'une association EIM permet d'associer un nom principal de service kerberos à un profil utilisateur i5/OS.

Indiquez le mot de passe à utiliser pour les noms principaux de service. Ce mot de passe doit être identique au mot de passe utilisé lors de la création des entrées de fichiers de clés et de la définition du nom principal dans le centre KDC.

Fichier de clés :

Principaux i5/OS

Mot de passe :

Confirmation du mot de passe :

< Précédent

Suivant >

Terminer

Annuler

Création des postes de fichier de clés (2)



LDAP peut utiliser kerberos pour authentifier des clients dans un environnement de connexion unique. Pour que cela soit possible, des postes du fichier de clés doivent être définis pour le service LDAP.

Indiquez le mot de passe à utiliser pour les noms principaux de service. Ce mot de passe doit être identique au mot de passe utilisé lors de la création des entrées de fichiers de clés et de la définition du nom principal dans le centre KDC.

Fichier de clés : /QIBM/UserData/OS400/NetworkAuthentication/krb5.keytab

Noms principaux LDAP

ldap/mante.notos.beaulieu@NOTOS.BEAULIEU

Mot de passe :

Confirmation du mot de passe :



Le serveur HTTP peut utiliser kerberos pour authentifier des clients dans un environnement de connexion unique. Pour que cela soit possible, des postes du fichier de clés doivent être définis pour le service HTTP.

Indiquez le mot de passe à utiliser pour les noms principaux de service. Ce mot de passe doit être identique au mot de passe utilisé lors de la création des entrées de fichiers de clés et de la définition du nom principal dans le centre KDC.

Fichier de clés : /QIBM/UserData/OS400/Network/

Principaux HTTP

HTTP/mante.notos.beaulieu@NOTOS.BEAULIEU

Mot de passe :

Confirmation du mot de passe :



Le système NFS peut utiliser kerberos pour authentifier des clients dans un environnement de connexion unique.

Indiquez le mot de passe à utiliser pour les noms principaux de service. Ce mot de passe doit être identique au mot de passe utilisé lors de la création des entrées de fichiers de clés et de la définition du nom principal dans le centre KDC.

Fichier de clés : /QIBM/UserData/OS400/NetworkAuthentication/krb5.keytab

Noms principaux System i NFS

nfs/mante.notos.beaulieu@NOTOS.BEAULIEU

Mot de passe :

Confirmation du mot de passe :

< Précédent Suivant > Terminer Annuler

NetServer

- Support de HOST et CIFS
- Nom court, nom long (FQDN), @IP, Qxxx



i5/OS NetServer peut utiliser kerberos pour authentifier des clients dans un environnement de connexion unique.

Indiquez le mot de passe à utiliser pour les noms principaux de service. Ce mot de passe doit être identique au mot de passe utilisé lors de la création des postes de fichiers de clés et de la définition du nom principal dans le centre KDC.

Fichier de clés :

Noms principaux i5/OS NetServer

```
HOST/mante.notos.beaulieu@NOTOS.BEAULIEU
cifs/mante.notos.beaulieu@NOTOS.BEAULIEU
HOST/mante@NOTOS.BEAULIEU
cifs/mante@NOTOS.BEAULIEU
HOST/qmante@NOTOS.BEAULIEU
cifs/qmante@NOTOS.BEAULIEU
HOST/192.168.1.3@NOTOS.BEAULIEU
cifs/192.168.1.3@NOTOS.BEAULIEU
```

Mot de passe :

Confirmation du mot de passe :

< Précédent

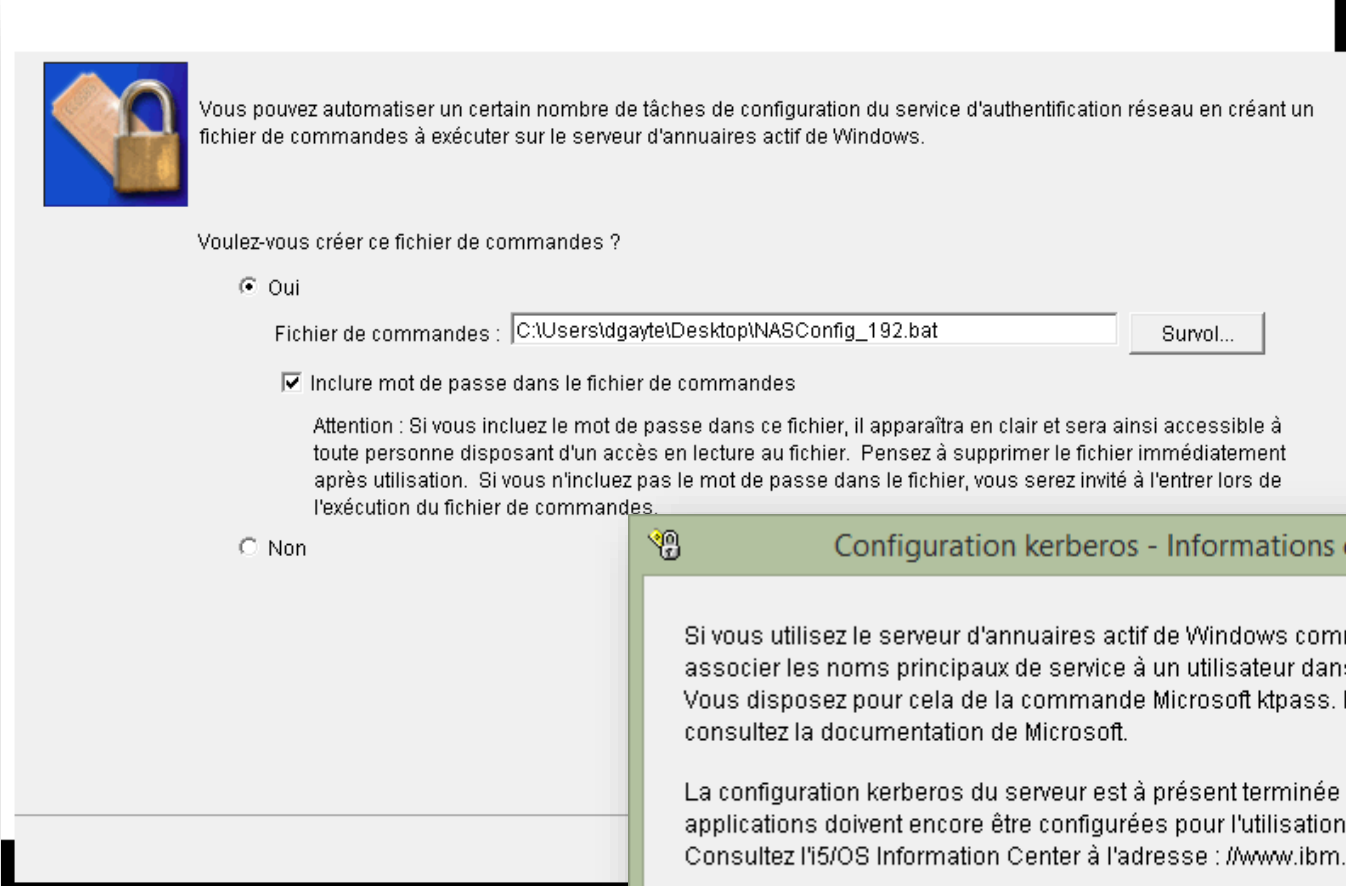
Suivant >


Terminer

Annuler

Création du fichier de commandes

- Simplifie la création des comptes de l'AD



 Vous pouvez automatiser un certain nombre de tâches de configuration du service d'authentification réseau en créant un fichier de commandes à exécuter sur le serveur d'annuaires actif de Windows.

Voulez-vous créer ce fichier de commandes ?

Oui

Fichier de commandes :

Inclure mot de passe dans le fichier de commandes

Attention : Si vous incluez le mot de passe dans ce fichier, il apparaîtra en clair et sera ainsi accessible à toute personne disposant d'un accès en lecture au fichier. Pensez à supprimer le fichier immédiatement après utilisation. Si vous n'incluez pas le mot de passe dans le fichier, vous serez invité à l'entrer lors de l'exécution du fichier de commandes.

Non

Configuration kerberos - Informations complémentaires

Si vous utilisez le serveur d'annuaires actif de Windows comme centre KDC, vous devez associer les noms principaux de service à un utilisateur dans ce serveur d'annuaires actifs. Vous disposez pour cela de la commande Microsoft ktpass. Pour plus d'informations, consultez la documentation de Microsoft.

La configuration kerberos du serveur est à présent terminée ; cependant, la plupart des applications doivent encore être configurées pour l'utilisation de l'authentification kerberos. Consultez l'i5/OS Information Center à l'adresse : [/www.ibm.com/eserver/series](http://www.ibm.com/eserver/series).

Le fichier de commande

```
DSADD user cn=mante_1_krbsvr400,cn=users,dc=NOTOS,dc=BEAULIEU -pwd Monpwd14 -display mante_1_krbsvr400  
KTPASS -MAPUSER mante_1_krbsvr400 -PRINC krbsvr400/mante.notos.beaulieu@NOTOS.BEAULIEU -PASS Monpwd14 -mapop set +DesOnly -ptype KRB5_NT_PRINCIPAL
```

■ Ajout d'une Unité d'Organisation

```
DSADD user cn=mante_1_krbsvr400,OU=Mante,OU=EIM,dc=NOTOS,dc=BEAULIEU -pwd Monpwd14 -display mante_1_krbsvr400  
KTPASS -MAPUSER mante_1_krbsvr400 -PRINC krbsvr400/mante.notos.beaulieu@NOTOS.BEAULIEU -PASS Monpwd14 -mapop set +DesOnly -ptype KRB5_NT_PRINCIPAL
```

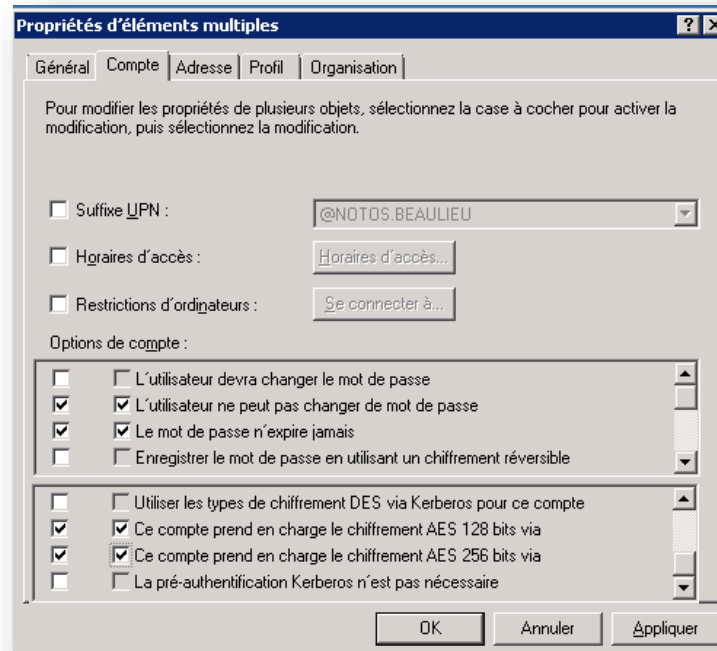
■ Selon les versions

- -mapop set +DesOnly à enlever (ou à ajouter dans les anciennes versions de l'IBM i)
- -ptype KRB5_NT_PRINCIPAL à ajouter

```
DSADD user cn=mante_1_krbsvr400,OU=Mante,OU=EIM,dc=NOTOS,dc=BEAULIEU -pwd Monpwd14 -display mante_1_krbsvr400  
KTPASS -MAPUSER mante_1_krbsvr400 -PRINC krbsvr400/mante.notos.beaulieu@NOTOS.BEAULIEU -PASS Monpwd14 -ptype KRB5_NT_PRINCIPAL
```


Modification des comptes

- Activer AES ou DES selon les versions d'IBM i
- Autoriser la délégation de compte
- Désactiver la péremption du mot de passe



Propriétés du NAS

- Utiliser TCP

Général | Résolution hôte | Total de contrôle | Tickets

Domaine par défaut : NOTOS.BEAULIEU

Protocole de communication pour le centre KDC

- Utiliser TCP
- Utiliser UDP

Options de centre KDC par défaut

- Renouvellement possible
- Transfert par proxy possible
- Réacheminement possible

Ecart horaire maximal : 300 secondes

OK Annuler Aide ?

Tests

- La configuration du NAS est terminée ! Il faut tester.
- Dans QSHELL (STRQSH) (première méthode)
- `keytab list` permet de voir les clés générées

```
> keytab list
  Key table: /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab

Principal: krbsvr400/mante.notos.beaulieu@NOTOS.BEAULIEU
  Key version: 1
  Key type: 56-bit DES
  Entry timestamp: 2014/04/29-15:12:10

Principal: krbsvr400/mante.notos.beaulieu@NOTOS.BEAULIEU
  Key version: 1
  Key type: 56-bit DES using key derivation
  Entry timestamp: 2014/04/29-15:12:10

Principal: krbsvr400/mante.notos.beaulieu@NOTOS.BEAULIEU
  Key version: 1
  Key type: 128-bit AES
  Entry timestamp: 2014/04/29-15:12:10
```

Validation

- Génération d'un ticket avec `kinit -k`
- Si cela fonctionne, la couche Kerberos est opérationnelle

```
> kinit -k nfs/mante.notos.beaulieu@NOTOS.BEAULIEU
$
```

- Le `$` signifie que tout est OK
- Sinon une erreur est signalée

```
kinit -k nfs/mante.notos.beaulieu@NOTOS.BEAULIEU
EUVF06014E Unable to obtain initial credentials.
                Status 0x96c73a34 - Response too large for datagram.
$
```

– Voir le status

Quelques erreurs

- EUVF06007E Unable to obtain name of default credentials cache.
 - L'utilisateur a t-il un répertoire personnel ? (/home/profilxx)
- EUVF06014E Unable to obtain initial credentials
 - Status 0x96c73a9c - Unable to contact security server.
 - Impossibilité de contacter le KDC
 - Status 0x96c73a25 - Time differential exceeds maximum clock skew.
 - Différence de temps trop importante entre le KDC et l'IBM I
 - Status 0x96c73a06 - Client principal is not found in security registry.
 - Erreur de syntaxe dans le nom du principal ou dans le nom de domaine
 - Status 0x96c73a9a - Unable to locate security server.
 - Problème dans le nom du realm (syntaxe ? Casse ?)

Seconde méthodes

- Il y a maintenant des commandes de l'IBM i à la place de QSHELL
- Ajouter un ticket
 - ADDKRBTKT
PRINCIPAL('nfs/mante.notos.beaulieu@NOTOS.BEAULIEU')
PASSWORD()
 - Voir la JOBLOG

```
ADDKRBTKT PRINCIPAL('nfs/mante.notos.beaulieu@NOTOS.BEAULIEU') PASSWORD()  
The ticket granting ticket has been created successfully.
```

- Si erreur

```
ADDKRBTKT PRINCIPAL('nfs/mante.notos.beaulie@NOTOS.BEAULIEU') PASSWORD()  
The initial credentials can not be obtained.
```

```
Message . . . . : The initial credentials can not be obtained.  
Cause . . . . . : An attempt was made to obtain an initial credentials, the  
Kerberos message: Client principal is not found in security registry with  
Kerberos error: X'96C73A06' was received. The following are possible causes  
that the operation was not successful:
```

Tickets

- Ils sont placés dans

/qibm/userdata/OS400/NetworkAuthentication/creds

- Surveiller leur nombre
 - Eventuellement les supprimer
 - DLTKRBCCF

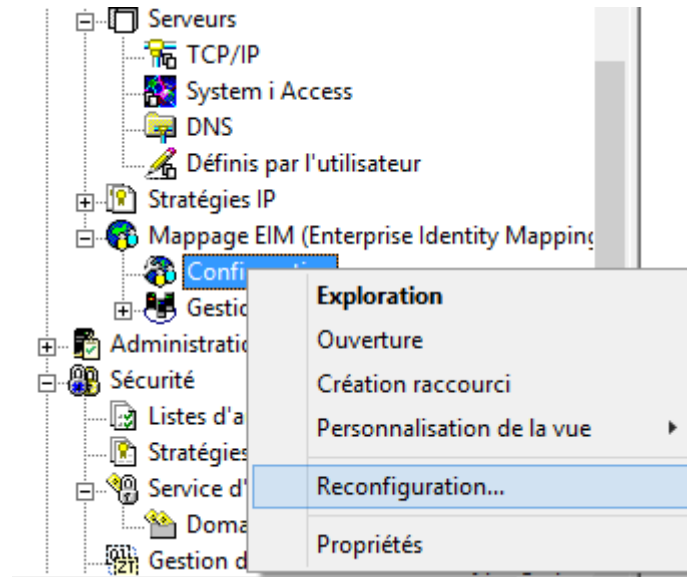
Opt	Lien objet	Type	Attribut	Texte
—	krbcred_0bcc3ac0	STMF		
—	krbcred_29e530a0	STMF		
—	krbcred_35fb19a0	STMF		
—	krbcred_35fb2550	STMF		

EIM : principes

- Association entre
 - Source (compte de l'AD)
 - Cible (profil utilisateur IBM i)
- S'appuie sur l'annuaire LDAP de l'IBM i
- Très souple
 - Pas de loi du tout ou rien
 - Chaque utilisateur peut participer (ou ne pas participer) à EIM

Assistant

- Dans IBM i Navigator/Réseau

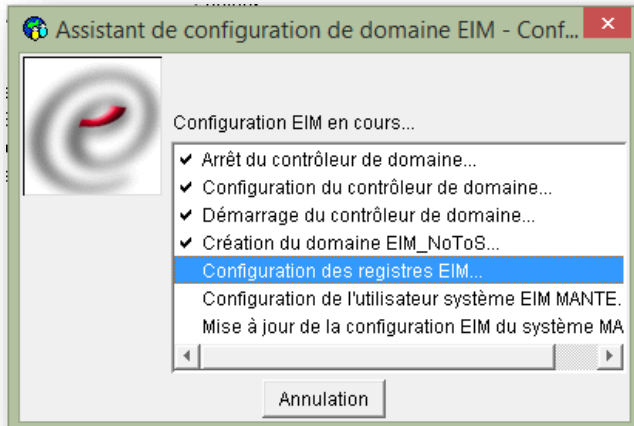


Assistant Configuration EIM

The image displays a sequence of five overlapping screenshots from the 'Assistant de configuration de domaine EIM' (EIM Domain Configuration Assistant) on an IBM i system. Each window has a title bar and a close button.

- Assistant de configuration de domaine EIM - Bienvenue**: Welcome screen. Text: 'Bienvenue dans l'assistant de configuration EIM (Enterprise Identity Mapping). Cet assistant vous aidera à configurer votre système afin qu'il soit intégré à un domaine EIM. Vous pouvez configurer votre système pour l'inclure dans un domaine existant ou créer et configurer un nouveau domaine EIM. Indiquez le type de configuration EIM que vous souhaitez pour votre système.' Options: 'Inclusion du système existant' (selected), 'Création d'un nouveau domaine EIM'. Buttons: 'Aide', '?'.
- Assistant de configuration de domaine EIM - Indication de l'emplacement du domaine EIM**: Text: 'Cet assistant vous aide à créer et à configurer un domaine EIM sur un serveur d'annuaires du réseau. Ce serveur d'annuaires deviendra le contrôleur de domaine pour votre nouveau domaine EIM. Vous pouvez configurer le serveur d'annuaires sur le système local, ou indiquer un serveur d'annuaires éloigné qui sera le contrôleur de domaine pour ce domaine.' Option: 'Sur le serveur local' (selected). Buttons: 'Aide', '?'.
- Assistant de configuration de domaine EIM - Utilisateur pour la connexion**: Text: 'Pour que l'assistant puisse terminer la configuration EIM, il doit être connecté au contrôleur de domaine avec un ID utilisateur admis. Quel ID utilisateur l'assistant doit-il utiliser?' Field: 'Type d'utilisateur : Nom distinctif et mot de passe'. Buttons: 'Aide', '?'.
- Assistant de configuration de domaine EIM - Domaine**: Text: 'Le domaine EIM est constitué d'un contrôleur de domaine et de registres utilisateur intégrés dans le réseau. Indiquez le nom du domaine à créer.' Fields: 'Domaine : EIM_NoToS', 'Description : Créé par l'assistant.' Buttons: 'Aide', '?'.
- Assistant de configuration de domaine EIM - Nom distinctif parent pour le domaine**: Text: 'Le nom distinctif (DN) parent définit plus précisément l'emplacement des données EIM dans l'annuaire. Souhaitez-vous indiquer un nom distinctif parent pour le domaine EIM ?' Options: 'Oui' (selected), 'Non'. Field: 'Nom distinctif parent :'. Button: 'Suiv...'. Buttons: 'Aide', '?'.
- Assistant de configuration de domaine EIM - Informations sur les registres**: Text: 'Les registres utilisateur constituent un ensemble de définitions utilisateur pour un système d'exploitation ou une application. Seuls les registres utilisateur qui ont été ajoutés au domaine EIM peuvent participer au mappage EIM. Les registres ci-après peuvent être utilisés par le système pour l'exécution de fonctions EIM au titre de fonctions du système d'exploitation.' Text: 'Indiquez les registres utilisateur qui vont être utilisés par le système local. Tout registre inexistant sera ajouté au domaine.' Options: 'i5/OS local' (checked), 'Kerberos' (checked). Fields: 'MANTE.NOTOS.BEAULIEU', 'NOTOS.BEAULIEU'. Option: 'Distinction majuscules/minuscules active pour les identités d'utilisateur kerberos' (unchecked). Button: 'Aide'.

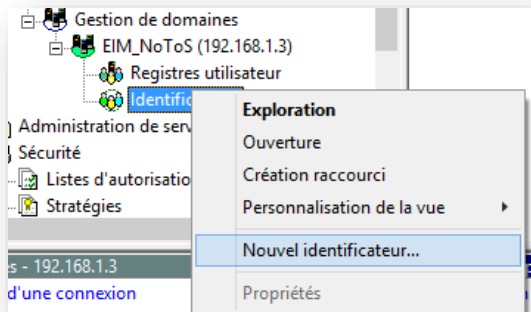
Création du domaine EIM



Environnement : Mes connexions		192.168.1.3: Configuration			
+	Configuration et maintenance				
-	Réseau				
+	Configuration TCP/IP				
+	Services d'accès à distance				
-	Serveurs				
	TCP/IP				
	System i Access				
	DNS				
	Définis par l'utilisateur				
+	Stratégies IP				
-	Mappage EIM (Enterprise Identity Mapping)				
	Configuration				
		Contrôleur de domaine	Local	Etat	Domaine
		MANTE.NOTOS.BEAULIEU	Oui	Démarré	EIM_NoToS

Création d'un identificateur

- Contiendra les associations cible et source



192.168.1.3: Identificateurs Inclusion : Tout	
Identificateur	Description
Dominique GAYTE	

Ajout d'association - Dominique GAYTE

Identificateur EIM :

Registre :

Utilisateur :

Type d'association :

Ajout d'association - Dominique GAYTE

Identificateur EIM :

Registre :

Utilisateur :

Type d'association :

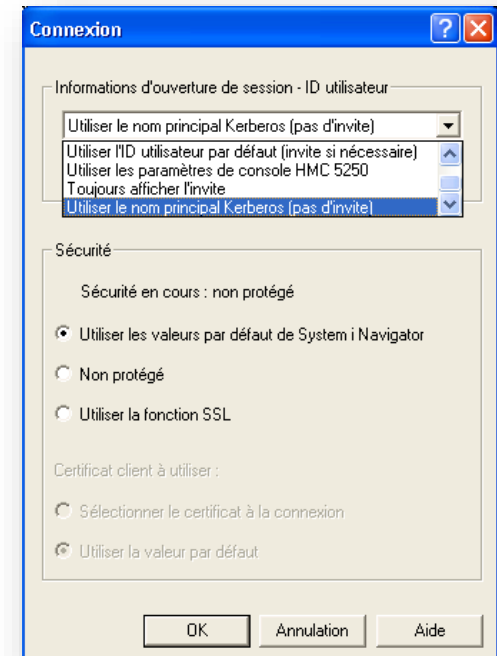
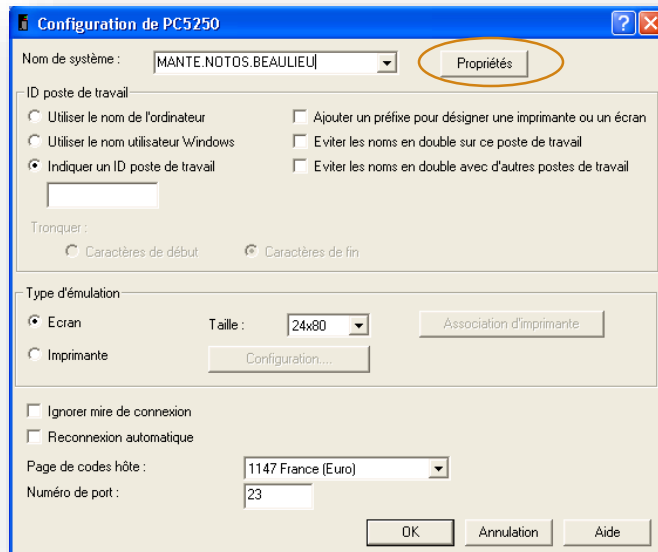
Emulation écran d'IBM i Access

■ Coté IBM i

- Valeur système QRMTSIGN à *VERIFY ou *SAMEPRF

■ Coté client

- Ouvrir une session Windows sur le domaine
- Modifier les propriétés de la connexion
 - Utiliser le nom principal Kerberos

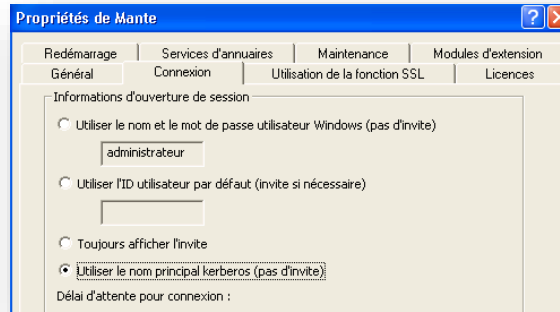


Emulation écran d'IBM i Access (2)

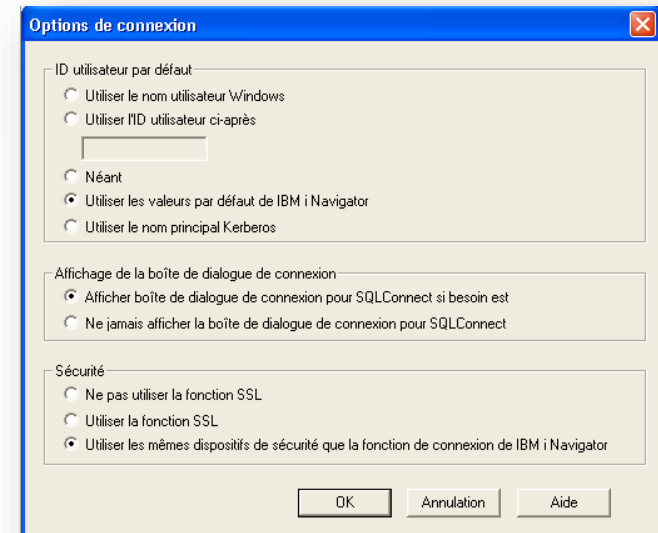
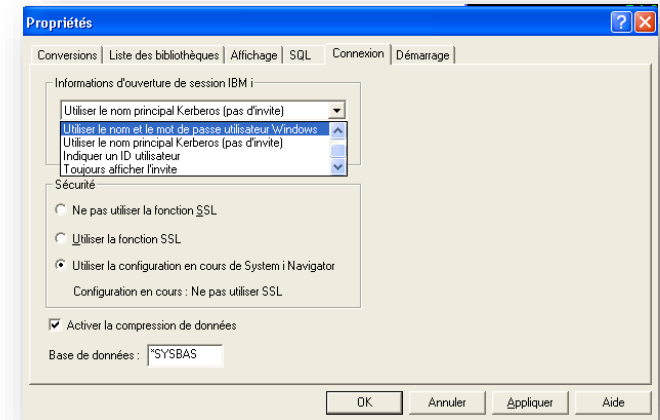
- Plusieurs sessions peuvent être configurées
 - Certaines en Kerberos
 - D'autres non Kerberos
- Les profils utilisateurs peuvent avoir PASSWORD(*NONE)
- En automatique prévoir la modification des fichiers CAE
[CAE]
UserIDSource=4

Autres fonctions d'IBM i Access

- Transfert de fichiers
- System i Navigator

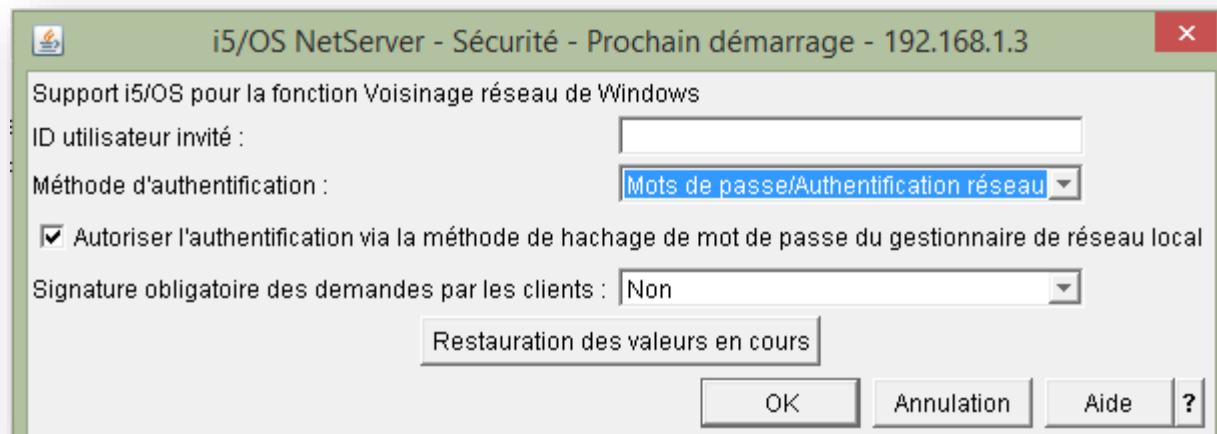


- ODBC/JDBC



NetServer

- Partage de fichiers et imprimantes de Windows
- Configurer le serveur i5 OS NetServer pour qu'il accepte Kerberos
 - Sécurité/prochain démarrage
 - Authentification réseau = Kerberos
 - Mixte avec « Mots de passe/Authentification réseau »
 - Redémarrer le serveur NetServer (attention aux connexions en cours!)



Autres serveurs supportés

- LDAP
- HTTP Server
- QNTC

Synthèse

- Très souple, ne peut concerner que certains utilisateurs
- Prend en compte la plupart des services (Telnet, transfert de fichiers, IBM i Navigator, NetServer, Web...)
- Mots de passe peuvent être à *NONE sur l'IBM i
- Création des identifiants EIM et des associations
 - En mode graphique
 - En partie (pas la source) en CL (xxxUSRPRF, paramètre EIMASSOC)
 - Par des API
- Penser aux procédures de reprise en cas de soucis avec l'AD



IBM Power Systems - IBM i

S28 - La mise en œuvre de SSO (*Single Sign On*) avec EIM (*Enterprise Identity Mapping*)

Merci de votre attention

Dominique GAYTE- dgayte@notos.fr
04 30 96 97 33
www.notos.fr

