

Sécuriser les applications et les données IBM i à partir de l'Active Directory

Dominique GAYTE
dgayte@notos.fr – www.notos.fr



NoToS - IDInfo

- Expertise autour de l'IBM i
- Sécurité
- PHP sur IBM i
- DB2 Web Query
- Développement de progiciels



lorena 

distant.backup 

monitor i 

power.gdpr 

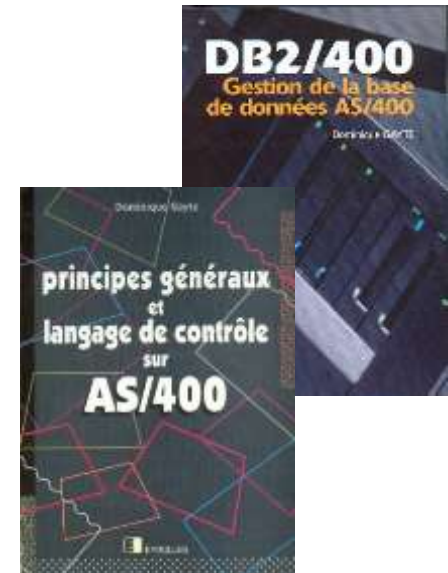
power.sign 

power.spool 

AD-ICT 

Dominique GAYTE

- Intervenant « AS/400 » depuis 1990
 - Au nom d'IBM
 - Plus de 1 000 journées au nom d'IBM
- Sécurité
 - Audit
 - Formation
 - Mise en œuvre : SSO, SSL, sécurisation de la base de données, RGPD...
- Développements complexes
 - Sécurité
 - Points d'exit (Power.exit)
 - AD-iCT
 - API système
 - RPG IV
 - XML
 - Accès bases de données distantes



Plan de la présentation

- Sécurité V7R4 : Philippe BOURGEOIS (IBM)
- Introduction
- Sécurisation des connexions à l'IBM i
 - SSO avec EIM
 - AD-iCT
- Sécurisation des applications et des données de l'IBM i
 - La problématique
 - Solution
 - Organisation proposée
 - AD-iCT



Introduction

Le contexte

- L'AD (Active Directory de Microsoft) est omniprésent dans les entreprises
- Il sert notamment à centraliser
 - Les authentifications dans le monde Windows
 - La gestion des habilitations de l'entreprise (messagerie, serveurs de fichiers, accès...)
- D'où les questions récurrentes

Comment peut-on s'appuyer sur l'AD pour sécuriser :

- Les connexions à l'IBM i
- Les données et les applications de l'IBM i ?



- L'idée est d'avoir un centre unique de gestion de la Sécurité et des habilitations qui serait l'AD

L'authentification

- Un SSO (Single Sign On) est une technologie permettant une authentification unique donnant un accès sur x systèmes/applications
- Sur IBM i, il existe un SSO avec l'AD s'appuyant sur EIM (*Enterprise Identity Mapping*)
- L'authentification est réalisée au niveau de l'AD seulement
 - Ce qui permet d'avoir une vraie politique de mot de passe
 - Complexité
 - Limitation dans le temps
 - Autres méthodes possibles
 - Carte à puce
 - Biométrie
 - ...
- L'IBM i fait confiance à cette authentification
 - Pas de mot de passe échangé
 - Seuls des tickets (Kerberos) cryptés circulent

Les habilitations

- Les habilitations définissent ce que chacun a le droit de faire
- Au niveau de Windows, elles sont gérées avec les groupes de Sécurité de l'AD
- L'idée est de s'appuyer sur ces groupes pour la Sécurité IBM i
- Assure une centralisation de la configuration
 - Plus de Sécurité
 - Plus d'organisation

Le SSO avec EIM

L'IBM i fait confiance à l'AD !



Principes

- L'authentification se fait au niveau de l'AD, pas de l'IBM i
 - Les profils utilisateurs peuvent avoir PASSWORD(*NONE)
- Permet une augmentation du niveau de Sécurité des mots de passe
 - Souvent une demande forte des auditeurs
- Simplicité d'accès pour les utilisateurs
 - Un seul mot de passe à retenir, celui de l'AD
- Suppression de l'écran d'ouverture (Telnet ou autres)
- Fini les soucis d'accès à l'IFS et de profils désactivés
- Fiable (fonctionne depuis plus de 15 ans)
- S'appuie sur des produits standards de l'IBM i et de Windows Server

Principes (2)

- Le SSO s'appuie sur 2 niveaux
 - Authentification avec Kerberos (Network Authentication Service)
 - Autorisation avec EIM (Enterprise Identity Mapping)

- L'IBM i fait confiance à l'authentification réalisée par Kerberos (l'AD)
 - Authentification réalisée lors de l'ouverture de la session Windows
 - Pas d'échange de mot de passe ultérieur

Configuration de Kerberos

- Via un assistant graphique
 - System i Navigator (à abandonner...)
 - Navigator for i (à privilégier)

- Génère
 - Des clés côté IBM i
 - Un fichier de commande (.BAT) à appliquer sur un contrôleur de domaine
 - Création d'une quinzaine de comptes de service

- La configuration du réseau doit être parfaite
 - Nommage de la partition
 - DNS et reverse
 - Horloges

Assistant Kerberos

- Dans la partie Sécurité

☐ Sécurité

- Listes autorisation
- Création liste autorisation
- Modification des droits sur les objets
- Administration des applications
- Gestion des clés des services de chiffrement
- Détection des intrusions

☐ Toutes les tâches

- Configuration
- Droits
- ☑ Gestion des clés des services de chiffrement
- ☐ Service d'authentification réseau
 - Configuration
 - Domaine
 - Gestion de fichier de clés
 - Propriétés
- ☑ Domaine

Configuration de service d'authentification réseau - localhost

Configuration du service d'authentification réseau - Informations sur le domaine

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



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

Domaine par défaut :


Microsoft Active Directory est utilisé pour l'authentification kerberos

< Précédent

Configuration de service d'authentification réseau - localhost

Configuration du service d'authentification réseau - Informations sur le centre KDC

Un centre KDC (Centre de distribution de clés) kerberos a deux fonctions. Il authentifie les principaux 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 :

< Précédent

Configuration de service d'authentification réseau - localhost

Configuration du service d'authentification réseau - Informations de serveur de mots de passe

Le serveur de mots de passe kerberos permet aux clients de modifier à distance leur mot de passe sur la même machine que le centre KDC.



Souhaitez-vous configurer ce système afin qu'il utilise un serveur de mots de passe pour le domaine ?

Oui

Serveur de mots de passe :

Port :

Non

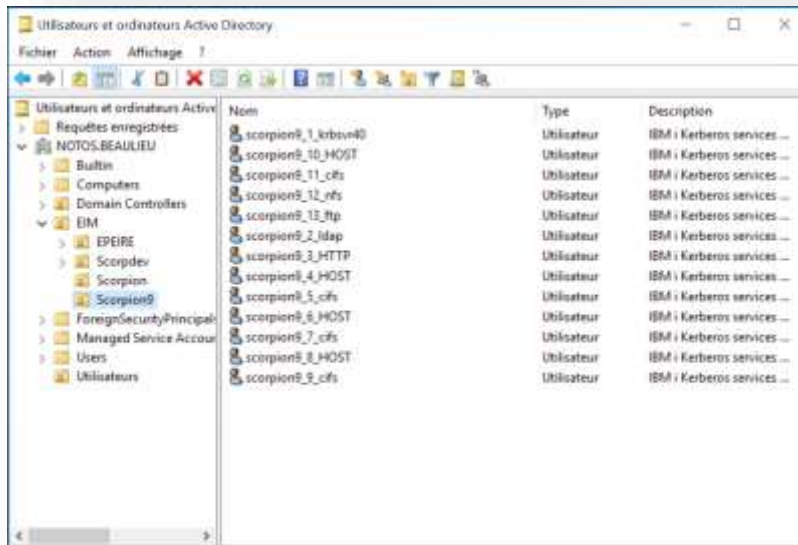
Kerberos coté AD

- Une quinzaine de comptes est créée à partir du fichier de commande généré

```
DSADD user "cn=scorpion9_1_krbsvr40,ou=Scorpion9,ou=EIM,dc=NOTOS,dc=BEAULIEU" -pwd M0nPwDxx -display scorpion9_1_krbsvr40 -pwdneverexpires yes -desc "IBM i Kerberos services on KTPASS -MAPUSER scorpion9_1_krbsvr40 -PRINC krbsvr40/scorpion9.notos.beaulieu@NOTOS.BEAULIEU -PASS M0nPwDxx -mapop set -crypto All -ptype KRB5_NT_PRINCIPAL
```

```
DSADD user "cn=scorpion9_2_ldap,ou=Scorpion9,ou=EIM,dc=NOTOS,dc=BEAULIEU" -pwd M0nPwDxx -display scorpion9_2_ldap -pwdneverexpires yes -desc "IBM i Kerberos services on system s KTPASS -MAPUSER scorpion9_2_ldap -PRINC ldap/scorpion9.notos.beaulieu@NOTOS.BEAULIEU -PASS M0nPwDxx -mapop set -crypto All -ptype KRB5_NT_PRINCIPAL
```

...



EIM : principes

- Association entre
 - Source (compte de l'AD)
 - Cible (profil utilisateur IBM i)
- S'appuie sur l'annuaire LDAP de l'IBM i
 - IBM Tivoli Directory Server for IBM i
- Très souple
 - Pas de loi du tout ou rien
 - Chaque utilisateur peut participer (ou ne pas participer) à EIM
 - On peut avoir des sessions SSO et non SSO sur le même poste. Par exemple
 - Une session Telnet SSO
 - Une session Telnet non SSO


Assistant EIM

- Dans Réseau

- [-] Réseau
 - [-] Configuration TCP/IP
 - [-] IPv4
 - Connexions IPv4
 - Interfaces IPv4
 - Routes IPv4
 - [-] IPv6
 - Lignes
 - [-] Serveurs
 - [-] Services accès à distance
 - [-] Stratégies IP
 - [-] EIM (Enterprise Identity Mapping)
 - Configuration
 - Gestion de domaines
- [-] Toutes les tâches
 - [-] Configuration TCP/IP
 - [-] Services accès à distance
 - [-] Serveurs
 - [-] Stratégies IP
 - [-] Internet
 - [-] IBM i NetServer
 - [-] EIM (Enterprise Identity Mapping)
 - Configuration
 - Gestion de domaines
 - [-] Configuration
 - Configuration
 - [-] Gestion de domaines

Assistant de configuration de domaine EIM - localhost

Assistant de configuration de domaine EIM - Bienvenue



Bienvenue dans l'assistant de configuration EIM (Enterprise Identity Mapping). à un domaine EIM. Vous pouvez configurer votre système pour l'inclure dans un domaine EIM.


Indiquez le type de configuration EIM que vous souhaitez pour votre système.

Inclusion du système dans un domaine existant
 Création d'un domaine et inclusion du système dans ce domaine

Vous pouvez cliquer à tout moment sur Annuler pour fermer l'assistant.

Assistant de configuration de domaine EIM - localhost

Assistant de configuration de domaine EIM - Indication de l'emplacement du domaine EIM




Cet assistant crée et configure un domaine EIM sur un serveur d'annuaire dans le réseau, votre nouveau domaine EIM. Vous pouvez configurer le serveur d'annuaire sur le système contrôleur de domaine pour ce domaine.

Indiquez l'emplacement de configuration de votre domaine EIM.

Sur le serveur d'annuaire local
 Sur un serveur d'annuaire éloigné

Assistant de configuration de domaine EIM - localhost

Assistant de configuration de domaine EIM - Utilisateur pour la connexion



Pour que l'assistant puisse terminer la configuration EIM, il doit être connecté au contrôleur de domaine. L'assistant doit-il utiliser ?

Type d'utilisateur : Nom distinctif et mot de passe ▼

Utilisateur

Nom distinctif :

Mot de passe :

Confirmation du mot de passe :

Création des associations

New EIM Identifier - EIM-NOTOS-BEAULIEU

Domain: EIM-NOTOS-BEAULIEU

Identifiant: Dominique GAYTE

Generate unique identifier

Description: Test Université IBM - 2019

Aliases

Alias: Add

Selection: Alias

Aucun

Page 1 de 1

Total : 0 Filtre : 0 Sélectionné : 0

OK Cancel

Add Association - Dominique GAYTE

EIM identifier: Dominique GAYTE

Registry: SCORPION9.NOTOS.BEAULIEU

User: DGAYTE

Association type: Target ▼

OK Cancel

Add Association - Dominique GAYTE

EIM identifier: Dominique GAYTE

Registry: NOTOS.BEAULIEU

User: Domi

Association type: Source ▼

OK Cancel

| Sélection | Registry | Registry Type | User | Association Type |
|-------------------------------------|-----------------------|---------------|--------|------------------|
| <input checked="" type="checkbox"/> | NOTOS.BEAULIEU | Kerberos | Domi | Source |
| <input type="checkbox"/> | SCORPION9.NOTO: IBM i | | DGAYTE | Target |

Services supportés

- Tout ce qui est Client Access et ACS
 - Émulation écran
 - ODBC/JDBC
 - Transfert de fichiers
- Partage de fichiers Windows (NetServer)
- HTTP Server (Web)
- FTP
- Accès Telnet/FTP entre partitions IBM i, LDAP, QNTC...

Mais...

- Interface graphique (Navigator for i) lourde et peu efficiente
 - Une quinzaine de clics par association par partition
- Répliquations non opérationnelles
 - Problématique dans le cadre de PRA/PCA
- Pas d'importation des associations en masse
- Pas de duplication des associations entre partitions
- Aucun outil d'analyse des données de l'EIM
 - Profils cibles inexistant
 - Sources en double
 - ...

AD-iCT : AD to i Communication Tools



- AD-iCT solution NoToS/IDInfo
- Saisie des associations déraisonnable pour plusieurs centaines d'utilisateurs
 - AD-iCT apporte l'automatisation et l'industrialisation d'un SSO basé sur EIM
 - AD-iCT est indispensable dans un environnement de production à partir de quelques dizaines de comptes
- Pour tout ce qui est interconnexion entre un IBM i et l'AD
 - Saisie en masse des identifiants
 - A partir d'un fichier (CSV, table) ou d'un écran vert
 - Réplication vers un autre système (backup, autres partitions de prod ou de dev...)
 - Les répliques habituelles ne fonctionnent pas
 - Souvent oublié dans les déploiements
 - Import/export
 - Et sécurisation à partir de l'AD (mais c'est le chapitre suivant)

AD-iCT : gestion des connexions interface 5250

```

DGAYTE                                     11/02/20
Webinar 11-02-2020      AD-iCT : Gestion des connexions      15:26:59
Indiquez vos options, puis appuyez sur ENTREE:
 1=Test Connexion 2=Modifier 3=Changer mot de passe 4=Supprimer 5=Afficher
 6=Exporter 7=Dupliquer 8=Identifiants 9=Intégrer BDD  A=Import IFS

Opt SERVEUR          LIBELLE          FQDN          Type
-  EPEIRE            IBM I POUR EIM EPEIRE      EPEIRE.NOTOS.BEAULIE  IBM I
-  FORMATION        Formation Sur Scorpion9    FORMATION.NOTOS.BEAU  IBM I
-  FRELON           FRELON AD WINDOWS         FRELON.NOTOS.BEAULIE  AD
-  SCORPDEV        SCORPDEV SUR SCORPION9    SCORPDEV.NOTOS.BEUL   IBM I
-  SCORPION9       IBM I POUR EIM SCORPION9  SCORPION9.NOTOS.BEAU  IBM I
-  SCORPXX         TEST NOTOS2 ET SCORPDEV   SCORPDEV.NOTOS.BEUL   IBM I

                                     Fin
F3=Exit  F6=Créer  F9=Backup EIM  F12=Précédent  F17=Langue  © NoToS 2019 2.0
    
```

AD-ICT : gestion des connexions interface Web

GESTION DES CONNEXIONS

Show entries

Search:

| SERVEUR ▲ | LIBELLÉ | FQDN | TYPE | ACTIONS | | | | | |
|-----------|--------------------------|--------------------------|-------|---------|--|--|--|--|--|
| EPEIRE | IBM I POUR EIM EPEIRE | EPEIRE.NOTOS.BEAULIEU | IBM I | | | | | | |
| FORMATION | Formation Sur Scorpion9 | FORMATION.NOTOS.BEAULIEU | IBM I | | | | | | |
| FRELON | FRELON AD WINDOWS | FRELON.NOTOS.BEAULIEU | AD | | | | | | |
| SCORPDEV | SCORPDEV SUR SCORPION9 | SCORPDEV.NOTOS.BEAULIEU | IBM I | | | | | | |
| SCORPION9 | IBM I POUR EIM SCORPION9 | SCORPION9.NOTOS.BEAULIEU | IBM I | | | | | | |
| SCORPXX | TEST NOTOS2 ET SCORPDEV | SCORPDEV.NOTOS.BEAULIEU | IBM I | | | | | | |

Showing 1 to 6 of 6 entries

Previous Next

AD-ICT : gestion des associations interface 5250

```

























DGAYTE                                     11/02/20
Webinar 11-02-2020                         Extraction des données EIM          15:28:16
SERVEUR: SCORPION9
Options : 2=Modifier, 4=Supprimer, 5=Afficher
Tous les identifiants
Identifiant à partir de :
Opt IDENTIFICATION      SOURCE          CIBLE          DESC
_ Angela Merkel         A.MERKEL       AMERKEL       Chancelier fédé
_ Boris Johnson         B.JOHNSON      BJOHNSON      Premier ministr
_ Démonstration        DEMONSTRATION  DEMO          Pour les démos
_ Démonstration Webinar WEBINAR        CIBLE
_ Donald Trump          DONALD.TRUMP   OTRUMP       Président des É
_ Elio Di Rupo         E.DI_RUPO      EIRUPO       Ministre-présid
_ GAYTE Dominique       DGAYTE         DGAYTE
_ Hery Rajaonarimampianina H.RAJAONARIMAMPIANIN HRAJAO       Président Madag
_ Justin Trudeau        J.TRUDEAU      JTRUDEAU     Premier ministr
_ Mahamadou Issoufou   M.ISSOUFOU    MISSOUFOU    Président de la
_ Marcelo Rebelo de Sousa M.REBELO_DE_SOUSA MDESUSA      Président de la
_ Mark Rutte            M.RUTTE        MRUTTE       Premier ministr
_ Martin Vizcarra      M.VIZCARRA     MVIZCARRA    Vice-président
_ Pas de source        [REDACTED]     DGAYTE       Manque cpt AD
                                                    A suivre...
F1=Codes couleurs      F3=Exit         F6=Créer      F11=Cibles inexistantes
F12=Précédent         F14=Suppression Masse  © NoToS 2019  2.0
    
```

AD-ICT : gestion des associations interface Web

– DONNÉES EIM –

NOM DU SERVEUR : SCORPION9 LIBELLÉ : IBM I POUR EIM SCC FQDN : SCORPION9.NOTOS TYPE : IBM I

Show 10 entries Search:

| IDENTIFICATION | SOURCE | CIBLE | DESCRIPTION | ACTIONS |
|---------------------|--------------------|-----------|--------------------|---|
| Pas de source | | DGAYTE | Manque cpt AD |   |
| Démonstration ... | WEBINAR | CIBLE | |   |
| ROEHRIG Yann-An... | YROEHRIG | YROEHRIG | |   |
| GAYTE Dominique | DGAYTE | DGAYTE | |   |
| Hery Rajaonarim... | H.RAJAONARIMAMP... | HRAJAO | Président Mada... |   |
| Angela Merkel | A.MERKEL | AMERKEL | Chancelier féd... |   |
| Donald Trump | DONALD.TRUMP | DTRUMP | Président des ... |   |
| Justin Trudeau | J.TRUDEAU | JTRUDEAU | Premier ministr... |   |
| Martin Vizcarra | M.VIZCARRA | MVIZCARRA | Vice-président... |   |
| Boris Johnson | B.JOHNSON | BJOHNSON | Premier ministr... |   |
| Vladimir Poutine... | V.POUTINE | VPOUTINE | Président de L... |   |
| Recep Tayyip Er... | R.ERDOGAN | RERDOGAN | Président de L... |   |

Les habilitations IBM i basées sur l'AD

Comment sécuriser les applications et les données IBM i à partir de l'AD

La demande

- Question récurrente des Services Informatique

Comment utiliser l'AD pour sécuriser les données et les applications IBM i ?

- Objectif : gestion unique des habilitations
 - Un seul endroit à gérer, un seul endroit à contrôler : l'AD
- Les habilitations sont réalisées au travers des groupes de Sécurité de l'AD

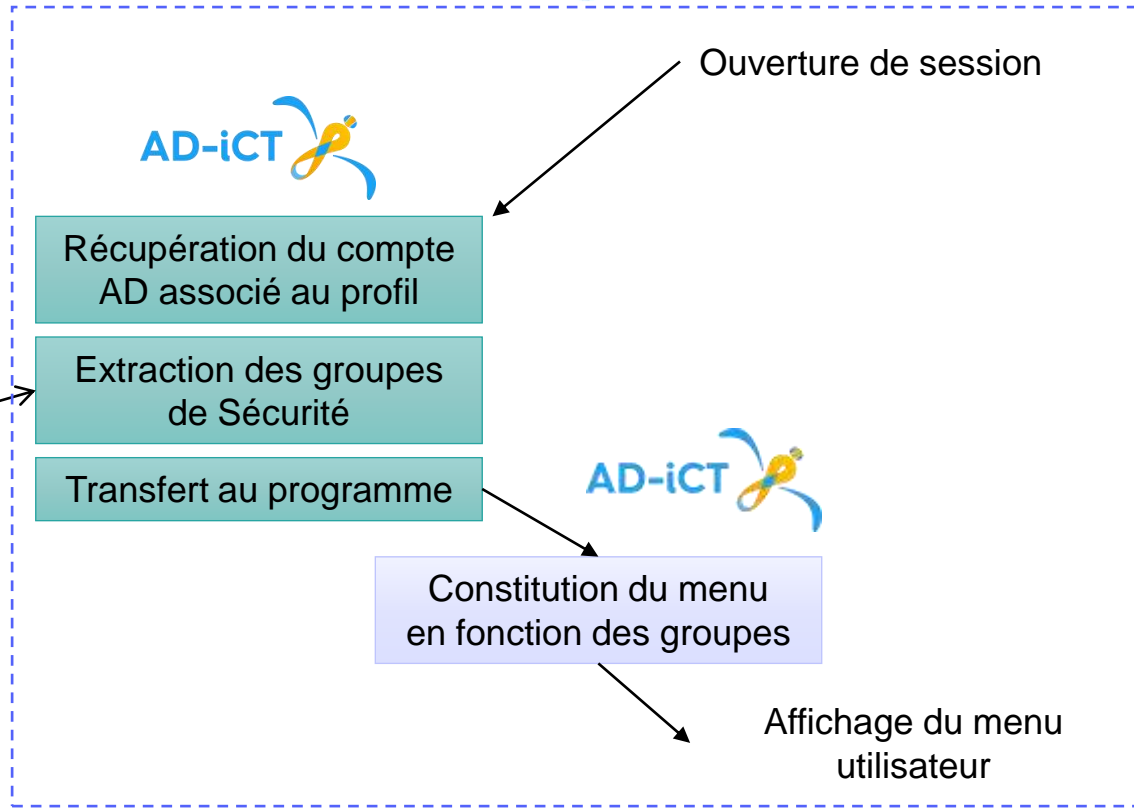
Les problématiques

- Un programme IBM i doit récupérer dynamiquement les groupes de Sécurité de l'AD auquel appartient un profil
 - Rien de trivial
- La Sécurité en place coté IBM i est souvent faible ou inexistante
 - Droits publics sur les objets (base de données !) en général *CHANGE ou *ALL
 - Profils utilisateur *ALLOBJ
- **AD Security for i est une composante d'AD-iCT**
 - Qui récupère en temps réel les groupes de sécurité d'un utilisateur
 - Et les mets à disposition des programmes IBM i (dans les structures de données)
 - Il permet aussi à un programme IBM i de vérifier si un utilisateur est associé à un groupe de sécurité de l'AD
 - Propose aussi un générateur de menu basé sur les groupes de Sécurité de l'AD (et d'autres mécanismes)

La structure applicative proposée

- Création d'un menu dynamique en fonction des groupes de Sécurité de l'AD
- Éventuellement vérification de l'appartenance à un groupe avant d'utiliser une fonction ou une ressource particulière
- Il faut pouvoir faire confiance à l'application IBM i
 - Pas de lignes de commandes
 - Droits des utilisateurs adaptés (pas de *ALLOBJ)

Schéma de l'organisation proposée



Sécurisation de la base de données : Idéalement :

- Droits publics : *EXCLUDE
- Propriétaire : *ALL
- Y a-t-il des accès directs ?
 - ODBC, JDBC, QUERY...
 - Utilisation d'un groupe LECTEUR (*USE)
 - Éventuellement d'un groupe MODIF (*CHANGE, à éviter)
- Utilisation recommandée d'une liste d'autorisation pour une gestion simplifiée
- NoToS/iDInfo vous accompagne dans cette démarche complexe

Les applications

- Tous les accès applicatifs se font par la délégation de droits
- Les programmes « points d'entrées » sont avec délégation de droits
 - USRPRF(*OWNER)
 - Propriétaire du programme = propriétaire des données
- Les autres programmes
 - USEADPAUT(*YES) qui est la valeur par défaut
 - Héritage de la délégation de droits du niveau supérieur

L'organisation pour une sécurité IBM i centrée sur l'AD

- Le SSO basé sur EIM doit être opérationnel
- L'AD doit être organisé avec des groupes de Sécurité (fonction standard)
- La sécurité de DB2 for i doit être renforcée
- Seuls les points d'entrée de l'application métier sont à revoir
 - Programme initial

AD-iCT



- AD to i Communication Tools
- Ensemble de fonctions qui facilitent l'intégration de l'IBM i dans un AD
- Objectif : renforcement de la Sécurité
- Trois composants
 - Tools for EIM
 - Gestion aisée et automatisée des identifiants EIM
 - Backup for EIM
 - Réplication des identifiants EIM entre différentes partitions IBM i
 - AD Security for i
 - Les applications IBM i traditionnelles s'appuient sur les groupes de Sécurité de l'AD pour la sécurisation des applications et des données
 - L'administrateur AD peut créer, modifier, supprimer des profils utilisateur et des associations EIM à partir de PowerShell
 - Générateur de menu automatique en fonction des groupes de sécurité auxquels appartient le compte AD/Profil utilisateur

AD-iCT (2)

- Ensemble d'objets
 - Programmes
 - Programmes de services, procédures et fonctions
 - Méthodologie
- A utiliser tel quel par vos équipes
- Ou intégré par nos collaborateurs lors des prestations de consolidation du niveau de Sécurité de vos systèmes



AD-ICT : gestion dynamique des menus à partir des groupes de Sécurité de l'AD

Le compte AD appartient au groupe Responsable des services financiers

```

DEMO
Webinar 11-02-2020      Liste des menus et options disponibles

Option  Libellé
D1      Distant Backup
P1      Paie
XX      Menu Inutilisable
02      Distant Backup
07      Administration Zend Server
08      Ressources Humaines
09      Fiche Client
10      Comptabilité
11      Logistique & Achat

Indiquer le numéro de l'option choisie :
F3=Exit
F12=Précédent
    
```

Propriétés de : Demonstration DEMO. Demonstration

Environnement Sessions Contrôle à distance Profil des services Bureau à distance COM+
 Général Adresse Compte Profil Téléphones Organisation Membre de Appel entrant

Membre de :

| | |
|--|--|
| Nom | Dossier Services de domaine Active Directory |
| DemoAD-ICT | NOTOS.BEAULIEU/Users |
| Responsable des services financiers... | NOTOS.BEAULIEU/Users |
| Utilisateurs du Bureau à distance | NOTOS.BEAULIEU/Builtin |
| Utilisateurs du domaine | NOTOS.BEAULIEU/Users |

Ajouter... Supprimer

Groupe principal : Utilisateurs du domaine

Définir le groupe principal Il n'est pas utile de modifier le groupe principal, sauf si vous disposez de clients Macintosh ou d'applications compatibles POSIX.

OK Annuler Appliquer Aide

AD-ICT : gestion dynamique des menus à partir des groupes de Sécurité de l'AD

Le compte AD n'appartient plus au groupe Responsable des services financiers

```

DEMO
Webinar 11-02-2020      Liste des menus et options disponibles
11 SC

Option  Libellé

XX  Menu Inutilisable
09  Fiche Client
10  Comptabilité
11  Logistique & Achat

Indiquer le numéro de l'option choisie :
F3=Exit          F12=Précédent  © NoToS 2019
    
```

Propriétés de : Demonstration DEMO. Demonstration

Environnement
 Sessions
 Contrôle à distance
 Profil des services Bureau à distance
 COM+

Général
 Adresse
 Compte
 Profil
 Téléphones
 Organisation
 Membre de
 Appel entrant

Membre de :

| | |
|-----------------------------------|--|
| Nom | Dossier Services de domaine Active Directory |
| DemoAD-ICT | NOTOS.BEAULIEU/Users |
| Utilisateurs du Bureau à distance | NOTOS.BEAULIEU/Builtin |
| Utilisateurs du domaine | NOTOS.BEAULIEU/Users |

Ajouter... Supprimer

Groupe principal : Utilisateurs du domaine

Définir le groupe principal

Il n'est pas utile de modifier le groupe principal, sauf si vous disposez de clients Macintosh ou d'applications compatibles POSIX.

OK Annuler Appliquer Aide



Dominique GAYTE
NoToS – www.notos.fr
dgayte@notos.fr – 06 30 17 02 55