

RDS 2012 R2 Remote Desktop Services RDSH – RDP remote App - Web Access RDWA sys 32 – Cours & TP -

RDS 2012 - Client Léger - Bureau à Distance Michel Cabaré - Ver 1.3 - mai 2016-

RDS 2012 accès intranetCours-Travaux pratiques

Michel Cabaré – Ver 1.3 – Mai 2016

<u>www.cabare.net</u> ©

TABLE DES MATIÈRES

Evolution TS 2003 en RDS 2012 R2	5
Les noms des Evolutions :	5
Versions RDP :	5
Principales fonctionnalités RDP :	7
Administration distante via RDP Terminal Server – bureau à Distance: Activer le Bureau à Distance sur Serveur 2012r2: Client RDP (bureau à distance) Quitter - Déconnecter – Se déconnecter Mises en Evidence Quitter / fermeture de session Mstsc.exe /admin Session Console Options du Bureau à Distance Pare-Feu et N° Port par défaut Modification Port 3389 du Bureau à Distance	9 9 10 11 12 12 13 16 17
Serveur RDS et Domaine	19
Schéma Configuration RDS	19
Schéma Configuration avec Gateway RDS	19
Groupe de Serveur 2012	20
Groupe de Serveur	20
Installation Rôle RDS Préconisations : Présentation des Rôles et Services de Rôle Remote Desktop: Assistant Déploiement infrastructure RDS Assistant Déploiement rapide – 1 serveur Gestionnaire de Serveur - Services Bureau à distance Questions 2008R2 disparues sous 2012 Authentification NLA Serveur de Licence Qui peut utiliser les services RDS Experience Utilisateur	21 21 23 23 25 26 26 26 28 28 28 29
Tester le Bureau à distance	31
1° connexion Bureau à Distance	31
Gérer les connexions en Cours (service bureau à distance)	32
Remote Desktop Shadowing	33
Remote Desktop Shadowing invite de commande	34
Mise en Evidence Remote-FX	35
Collections	36
Les Collections RDS 2012 :	36
Les Collections de session:	36
Les éléments d'une Collection:	37
Paramétrages simples d'une Collection:	38
Gestionnaire de Licences Importance Du Gestionnaire :	39 39 39



Ajour service de Rôle Gestionnaire de licence:	40
Paramétrage du Gestionnaire de licence:	43
Activation du Gestionnaire de licences:	43
Ajout dans Groupe de Sécurité Serveur de licence des services terminal Server:	:45
Id de serveur unique:	46
Migrer des licences :	47
Installer des licences :	49
Installer des licences :	51
Installer des applications sur le RDS	53
Installation d'applications Mode Execute - install	53
Commande Change user	53
Assistant Ajout programmes	54
Mode maintenance	55
Installer – publier – Distribuer	56
Programmes et Certificats	56
Profils Utilisateurs Les profils sur un serveur RDS : Objectif des profils itinérants : Les profils itinérants standards (rappel) : Les profils itinérants RDS par GPO Réglage GPO Profil itinérants problèmes réglages supplémentaires	57 57 58 59 60 63
UPD user Profils Disks UPD ou disques profils utilisateurs: Configuration minimale: Fichier UVHD-s1-xxxxx: Options UPD:	66 66 68 69
Applications et Remote App	70
Objectif des applications distantes Remote App :	70
Publication d'application Remote App :	70
Distribution d'application Remote App publiée:	71
Distribution portail RDWA	72
Groupe utilisateur du Bureau à distance (Vérification) :	72
Ajout Serveur RDS au Groupe Ordinateurs Serveur RDS endpoint (Vérification):	72
1° connexion Accès WEB https://UNCxxx/RDWEB :	73
Message Serveur de publication inconnu	74
Distribution fichiers RDP	75
Déploiements applications RemoteApp et .RDP:	75
Installation du certificat du portail WEB sur le client :	75
Paramétrage des connexions distantes du client windows :	77
Récupération des fichiers .rdp :	78
Utiliser les connexions distantes depuis windows 8.1 :	79
Utiliser les connexions distantes depuis windows 7 :	80
Portail RDWA Pré-requis navigateurs: Edge windows 10 (sans Activex) IE 10 et IE 11 + Activex sur windows 8.1 IE 9 + Activex Seven Navigateurs autres que IE: Firefox Présentation et Agencement du portail: Paramètres - propriétés Remote App :	81 81 82 83 84 85 87 87



Affichage dans des Dossiers	. 89
Création de bureau distants	. 90
Changer le titre du portail	. 92
PKI et Certificat	. 93
Besoin de certificats :	. 93
Types de Certificats et PKI	. 94
Déroulement gestion des certificats:	. 95
Création PKI de domaine:	.95
Ajout rôle Service de certificats AD	.95
Paramétrage du rôle Service de certificats AD	.97
Renouvellement PKI de domaine:	101
Déploiement - Quels Certificats pour Quels Serveurs:	103
Demande de création de Certificat de Domaine – via IIS:	104
Export de certificat:	107
Application / import de Certificat:	108
Application du Certificat sur IIS pour SSL (vérification) :	109
Vérification des Certificat	111
Connexion HTTPS au portail RDWeb –FQDN et domaine:	111
Connexion HTTPS depuis une machine hors domaine:	112
Editeur appli remoteApp inconnu Problème de Confiance dans l'éditeur des Applications : Empreintes numériques SHA1: GPO pour appliquer empreintes numériques:	113 113 113 113 114
SSo et Authentification	116
Double authentification :	116
Mise en œuvre de SSO Single Sign On :	117
EASY-PRINT	119
Principe des Impressions windows :	119
Principe des Impressions RDS :	120
Principe de Fonctionnement :	121
Visioneuse XPS :	121
GPO associées aux clients:	122
Annexe 1 – Configurations RDS	124
Configuration 1 serveur (+ licence) déploiement rapide :	124
Configuration 2 serveurs (+ licence) déploiement standard:	124
Configuration 3 serveurs (+ licence) déploiement standard :	125
Annexe2 – VM et conf Environnement Hyper-V Création d'une VM à partir d'un vhd existant 2 VM minimum, CD et RDS Montage du CD de domaine Ajout du rôle AD DS Configuration du Serveur Montage du RDS de domaine	126 127 129 129 129 132 134
Annexe 3 – installation office 2010	135
Message au 1° lancement d'office	135
Modèles de Stratégies office 2010	135
Installation d'office 2010 setup / admin	141
Annexe 4 – gestion Certificat	143
Console Certificats	143



EVOLUTION TS 2003 EN RDS 2012 R2

Les noms des Evolutions :

Terminal Server 2003 évolue depuis 2008 R2 en RDS Remote Desktop Server, du coup tous les services anciennement nommés TS.... deviennent RD...

l'objectif est d'évoluer dans le sens de la virtualisation du poste de travail (ou du client léger) ce qui chez microsoft prends le nom de **VDI Virtualisation Desktop Infrastructure**.

Dans la version suivante des Services 2016, qui sera peut être nommée Windows Cloud Services... ce sera surtout Hyper-V qui sera modifié...

Versions RDP :

RDP peut fournir le bureau complet, (bureau à distance) ou uniquement les applications choisies (**Remote Application**)

Le protocole RDP n'envoie à travers le réseau que les modifications d'écran, s'il n'y a pas de changement à l'écran, l'utilisation de la bande passante est nulle. Par exemple, lorsque la souris se déplace, on n'envois que le pointeur de la souris comme mise à jours d'écran...)

Pour connaître la version de RDP il suffit de demander "**A propos**" via le menu contextuel sur la boite de dialogue **Tous les programmes / Accessoires / Connexion Bureau à distance**

Version RDP	
Connexion Bureau à distance	Connexion Bureau à distance Connexion Bureau à distance Version du noyau 6.1.7601 Version de contrôle 6.1.7601 © 2007 Microsoft Corporation. Tous droits réservés.
Ordinateur : Exemple : computer.fabrikam.com Nom Aucun paramètre n'a été spécifié. d'utilisateur : Le champ du nom de l'ordinateur est vide. Entrez un nom complet d'ordinateur distant.	Authentification au niveau du réseau prise en Protocole RDP (Remote Desktop Protocol) 7.1 pris
Options Connexion Aide	

Version 5.1 avec Windows XP Pro

Changement des Terminal Services Client en Remote Desktop Connection. L'executables est tpoujours nommé mstsc.exe.

• support for 24-bit color et son

Version 5.2 (avec Windows Server 2003)

- support for console mode connections, a session directory,
- local resource mapping.
- Transport Layer Security (TLS) 1.0 for server authentication

Version 6.0 avec Vista 2003 Sp1, sous Xp sp2 et mac Os10



- , NLA Network Level Authentication
- multi-monitor spanning and large desktop support •

Version 6.1 avec windows 2008, (client xp sp3 minimum)

- connecting remotely to individual programs
- client-side printer redirection system •

Version 7.0 avec 2008 R2, 7, Xp sp3 ..

- Windows Media Player redirection, bidirectional audio, •
- multi-monitor support, enhanced bitmap acceleration, •
- Easy Print redirection •

Version 7.1 avec 2008r2 sp1, (client 7 sp1 minimum)

RemoteFX functionality. •

Version 8.0 (avec windows 8 windows 2012)

- Adaptive Graphics, DirectX 11 •
- automatic selection of TCP or UDP as transport protocol,

Version 8.1 avec Windows 8.1 and Windows Server 2012 R2. (client 7 sp1 mini)

Mise à jour pour RDP 8.1 est disponible pour Windows 7 SP1 https://support.microsoft.com/fr-fr/kb/2923545 •

10 avr. 2015 - Décrit une mise à jour pour 8.1 RDP dans Windows 7 SP1 et Windows Server 2008 R2 SP1.

💽 Windows6.1-KB2923545-x64.msu Il suffit d'installer

- Session shadowing
- "restricted admin" mode.

Version 10.0 avec windows 10 (and patch sever 2012 server 2016)

- AutoSize zoom (HiDPI clients)
- graphics compression H.264/AVC





Principales fonctionnalités RDP :

Remote FX est le nom donné à l'affichage en HQ à l'écran, II est désormais possible de voir un film en HD via un RDS hébergé qui plus est sur une machine Virtualisée en Hyper-V, à condition que le serveur qui héberge RDS ait une bonne carte graphique...

Les services qui apparaissent pour une utilisation simple de RDS sont

RD Remote Application - Remote App :

Pour donner l'accès aux applications sans passer par le bureau à distance. On envois via le protocole RDP uniquement l'application, sans construire tout le bureau à distance. C"est très simple pour l'utilisateur, qui ne se mélange plus les idées entre son bureau "normal" et son "bureau à distance"... Cela nécessite d'utiliser **Internet Explorer** comme navigateur car on utilise un **ActiveX**.

On retrouve la même philosophie que chez Citrix...

RDWA ou RD Web Access :

On arrive sur une page Web, sur laquelle nos applications sont disponibles... cela permet de simplifier la vie au client qui n'a plus à chercher son application voire a se promener sur un autre bureau. l'outils de "navigation reste le browser avec simplement une URL d'un intranet...

RDG ou RD Gateway :

Rend accessible un serveur RDS à travers HTTPS, donc sans tunnel VPN...

Sous 2003 pour rendre un serveur TSE disponible à distance il fallait

- 1. monter un VPN
- chercher le serveur TSE via une @ip privée en interne (on ne peut pas toujours faire un VPN, cela peut bloquer lorsque l'on utilise une liaison wifi publique, si les pare-feu n'ouvrent pas les bons ports...

Avec 2012 (et depuis 2008) on utilisera https, cela marchera tout le temps car on fait du RDP encapsulé dans du HTTPS, et le HTTPS est en général "ouvert" partout.



RD Easy Print :

Permet de ne pas avoir à installer les pilotes d'imprimante sur le serveur

Sous 2003 il fallait obligatoirement installer toutes les imprimantes sur le serveur TSE, ce qui pouvait parfois poser quelques soucis, (vieux drivers, driver 32bits...) voire être impossible

Depuis 2008R2, lorsque l'on imprime, on génère un fichier d'impression XPS (équivalent microsoft du format PDF...) Ce fichier ensuite est envoyé au client TS. On peut donc dire que si le client à une imprimante correctement installée el local, il doit pouvoir par ailleurs imprimer des fichier XPS (tout comme des PDF...)



ADMINISTRATION DISTANTE VIA RDP

Terminal Server – bureau à Distance:

Le principe est le même, on utilise en effet le protocole **RDP Remote Desktop Protocol** pour accéder à une machine distante. Quelques règles pour se repérer :

- Sous 2012r2 et 2008r2 SRV : il faut activer simplement le paramètre Bureau à distance
- Sous 2003 SRV : Si les services Terminal Server sont déjà opérationnels, il n'y à pas à activer le Bureau à Distance

Activer le Bureau à Distance sur Serveur 2012r2:

Dans le gestionnaire de serveur, serveur local on à tout de suite accès au Bureau à distance

a	Gestionnaire de serveur							
Gestionnaire de serveur • Serveur local • 🗇 l 🏲 🛛 🖓 🖓 🖓 Gérer								
Tableau de bord	PROPRIÉTÉS Pour srv-v							
Serveur local Tous les serveurs	Nom de l'ordinateur Domaine	srv-v cabare-intra.net	Dernières mise: Windows Upda	s à jour instal te	lées			
 Hyper-V Services de fichiers et d b 			Dernière recher	rche de mises	à jour :			
	Pare-feu Windows Gestion à distance Bureau à distance	Domaine : Inactif Activé Activé	Rapport d'erreu Programme d'a Configuration c	urs Windows mélioration d le sécurité re	de l'expéri nforcée d'			
	Association de cartes réseau	Désactivé	Fuseau horaire					

Donnant

Propriétés sys	tème	×	
Nom de l'ordinateur	Matériel		
Paramètres système avancés	Utilisation à distance		
Assistance à distance			
Autoriser les connexions d'assistance à	distance vers cet ordinateur		
	Options avancées		
			A priori si on veut se laisse
Bureau à distance			la possibilité d'administre
Choisissez une option, puis spécifiez qui pe	eut se connecter.		le serveur depuis des
) Ne pas autoriser les connexions à dista	nce à cet ordinateur		postes XP ou Seven, il fau
			demander n'importe
Autonser les connexions a distance a c	et ordinateur		quelle version du Bureau à
N'autoriser <u>que</u> la connexion des on à distance avec authentification NL	dinateurs exécutant le Bureau A (recommandé)		distance
Comment choisir ?	électionnez des utilisateurs		Si NLA cela implique ur
			client Seven Sp2 mini
OK	Annular Analian		
OK	Annuler Applique		

N.B: la méthode depuis 2008, reste valable... via les propriétés de Ordinateur, via Paramètres d'utilisation à distance, dans l'onglet Utilisation à Distance



Client RDP (bureau à distance)

Le fichier executable client rdp est mstsc.exe

Depuis windows 10 ou 8.1 il faut effectuer une recherche, via **cortana** ou la Recherche



On peut bien sur le poser sur le bureau, l'épingler à la barre des tâches, l'épingler sur l'écran d'accueil...

Depuis un poste Seven, on demande plutôt

programmes / accessoires / outils de communication / Connexion Bureau à distance



On peut utiliser un nom machine, une adresse Ip (si non membre d'un domaine) ou un FQDN (mieux)





L'authentification est demandée, puis la connexion effectuée



L'ouverture de session amène:



Quitter - Déconnecter - Se déconnecter

Il ne faut jamais **quitter une session** en fermant la fenêtre...





Si on ferme cette fenêtre, lors de la réouverture de la prochaine session on retrouvera le bloc note en... l'état ! Il faut plutôt fermer la session à distance proprement sur le serveur... via Démarrer, Arrêter ou se déconnecter / Se déconnecter

Explorateur de fichiers Rechercher Exécuter	Déconnecter Se déconnecter Arrêter	•	Se déconnecter = fin de session sur le poste distant
Arrêter ou se déconnecter	Redémarrer		Déconnecter = coupure de session distante



RDS 2012 R2 – accès intranet - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 11 - Michel Cabaré -

Mises en Evidence Quitter / fermeture de session...

N.B: Si une session locale est déjà ouverte sur le serveur sur lequel on prend la main avec le bureau à distance et sous un compte homonyme, alors cette session locale est déconnecté. C'est le fonctionnement par défaut.

Un petit essai pour mettre en évidence la différence entre **Se déconnecter** (fermer session) / **Déconnecter** (fermer la fenêtre...)

- 1. sur un poste sur lequel on a activé le bureau à distance, on ouvre une session locale en tant qu'administrateur, et on lance le bloc note...
- 2. depuis un client on tente une connexion RDP avec le même compte administrateur..., lorsque la session à distance est prise, on voit sur le poste la session en cours se fermer...
 - Si on ferme le bureau à distance par la croix de la fenêtre, on quitte le bureau à distance, mais la session reste "ouverte" sur le poste... Si on ré-ouvre la session "apparemment fermée", on retrouvera notre application

- H 🖬 🛋 Gestionnastv-vle serveur		- 6	×			
			Sa	ns titre - B	loc-notes	 ×
	Fichier cgvjbo yghij	Edition fjhc ftyj	Format	Affichage	?	^

• Si on ferme le bureau à distance en se déconnectant, Si on réouvre une session on ne retrouve plus rien...

Mstsc.exe /admin Session Console

On appelle "session console" la session qui est utilisée par défaut par le système pour envoyer les informations à l'écran.

On peut récupérer depuis n'importe quel poste cette session console, en se loguant avec l'option **/admin** du client bureau a distance. Et ce depuis le client 6.1 minimum. (avant on utilisait **/console**...)

Donc en invite de commande via



C:\Users\Administrateur.CABARE-INTRA>mstsc.exe /admin

N.B: Si un membre du groupe Administrateurs démarre une session Bureau à distance à un serveur Windows Server 2012, sur lequel le service de rôle de Terminal Server installé, ils doivent utiliser l'option **/admin** pour se connecter à une session pouvant administrer à distance le serveur

C'est la Session dite "session 0" (output std) et non pas la session TSE

Cette "session 0" à plusieurs caractéristiques :

- Elle ne consomme pas de "CAL"
- Elle n'est pas bloquée par un éventuel mode "maintenance" du serveur



Options du Bureau à Distance

Il est possible de modifier un certain nombre d'options lors de la demande de connexion sur le poste distant, via **Option**

🐮 Connexia	on Bureau	ı à distance			×			
-	Burea Coni	u à dista nexion	nce					
Ordinateur :	srv-dc1		i	~				
	Connex	ion Annul	er Aide	Options >>		ffiche	r les d	ontions
					00 A		103 (
		🎭 Connexi	ion Bureau à dista	nce	-		×	
		N	Connexior A distar	n Bureau 1Ce	I			
		Ordinateur :	srv-v			•		
		Nom d'utilisateur : Vos informati session Wind	TRAVAIL-10\Adm ons d'identification o lows seront utilisées	iinistrateur d'ouverture de pour la conne	ion.			
		Afficher	les options		Connexion	Ai	ide	

On peut atteindre différents onglets

Onglet général

Permet notamment de définir une machine cible et un utilisateur spécifique, et d'enregistrer à terme toute la configuration dans un fichier **.rdp**

Général A Paramètre	ffichage Ressources locales Expérience Avancé s d'ouverture de session Entrez le nom de l'ordinateur distant.				
	Ordinateur : srv-v ~				
	Nom d'utilisateur : TRAVAIL-10\Administrateur				
Vos informations d'identification d'ouverture de session Windows seront utilisées pour la connexion.					
	Vos informations d'identification d'ouverture de session Windows seront utilisées pour la connexion.				
	Vos informations d'identification d'ouverture de session Windows seront utilisées pour la connexion.				
Paramètre	Vos informations d'identification d'ouverture de session Windows seront utilisées pour la connexion. Toujours demander les informations d'identification s de connexion				
- Paramètre	Vos informations d'identification d'ouverture de session Windows seront utilisées pour la connexion. Toujours demander les informations d'identification s de connexion Enregistrez les paramètres de connexion actuels dans un fichier RDP ou ouvrez une connexion enregistrée.				



Pour se connecter avec ces valeurs de paramètres, il suffit de double cliquer dessus. Pour modifier ultérieurement ce fichier , il faut demander cli droit Modifier





Onglet Affichage

Permet de gérer l'interface graphique

Général	Affichage	Ressources locales	Expérience	Avancé			
Configuration de l'affichage							
2	Choisiss curseur	Choisissez la taille de votre Bureau à distance. Déplacez le curseur à l'extrême droite pour utiliser la totalité de l'écran.					
	Petit	Petit Grand					
		Plein écran					
	Utilis	er tous les moniteurs p	our la session	à distance			
Couleur	s						
	Choisir l'	Choisir l'intensité de la couleur de la session à distance.					
	Qualité	optimale (32 bits)	\sim				
Affich	er la barre de	e connexion en cas de	e mode plein é	cran			

Onglet Ressources locales

Permet de définir la redirection de lecteurs réseaux ou de ports USB...

Général A Sortie aud	ffichage Ressources locales io de l'ordinateur distant Configurer les paramètres au Paramètres	Expérience Avancé dio de l'ordinateur distant.	
Clavier	Appliquer les combinaisons o En mode plein écran unique	de touches Windows : ement ~	Passa mas et périphériques lacaure
Ressource	Exemple : ALT+TAB es et périphériques locaux		Choisissez les périphériques locaux Choisissez les périphériques et les ressources de cet ordinateur que vous souhaitez utiliser dans la session à distance.
20	Choisissez les périphériques souhaitez utiliser dans la ses Imprimantes Autres	et les ressources que vous sion à distance. Presse-papiers	Cartes à puce Ports Cartes à puce Cartes à puce Cartes périphériques Plug-and-Play (PnP) pris en charge Périphériques que je branche plus tard

Par exemple, si on se trouve sur un Poste et que l'on souhaite que son disque dur local soit "mappé" sur le poste auquel on accède a distance, il suffit de et les clés USB insérées localement demander au départ

✓Cartes à puce	✓Cartes à puce
Ports	Ports
Lecteurs	Lecteurs
Lecteur de disquettes (A:)	🖃 🗹 Autres périphériques Plug-and-Play (PnP) pris en charge
🗹 os-win10-1511 (C:)	🏹 Périphériques que je branche plus tard
data (D:)	A Company of the second

On aura un message de mise en garde ...

– SYS 32 – Cours TP - ver 1.3 -

Nonr 💀	nexion Bureau à distance	×		
1	npossible d'identifier l' raiment vous y connec	éditeur de cette connexion à distance. Voulez-vous ter ?		
Cette connexion distante peut endommager votre ordinateur local ou distant. Ne vous connectez pas, sauf si vous connaissez l'origine de cette connexion ou si vous l'avez déjà utilisée.				
	Éditeur :	Serveur de publication inconnu		
<u>_</u> ~	Type :	Connexion Bureau à distance		
	Ordinateur distant :	srv-v		



Et sur la machine distante on aura

Pour le disque	pour la clé usb
4 📕 Ce PC	Ce PC
D 📔 Bureau	E. Bureau
C sur TRAVAIL-10	Documents
👂 📗 Documents	🛖 F sur TRAVAIL-10

Onglet Programmes

Permet de démarrer un batch ou programme spécifique

Général	Affichage	Ressources locales	Programmes	Expérience	<u> </u>	>	
Démarrer un programme							
Démarrer le programme suivant lors de la connexion :							
Chemin d'accès au programme et nom du fichier :							
Démarrer dans le dossier suivant :							

Dans l'Onglets Experience on choisit une vitesse ou non



Dans l'onglet Avancé rien d'indispensable dans un premier temps



Pare-Feu et N° Port par défaut

Si on laisse Windows activer les réglages pour autoriser le Bureau à distance dans le pare-feu incorporé d'un Windows 10



Alors on observe que Bureau à distance par défaut n'ets pas accessible depuis un profil de réseau public

Domaine	Domestique/entreprise (. Public
Domaine	Domestique/entreprise (. Public
utilis 🗌		
VSD)		
P) 🗆		
HTTPS)		
	(utilis VSD) P) HTTPS) 2	L L (utilis] VSD)] P)] HTTPS)] V V V U U U U U U U U U U U U U

Cela correspond dans les **Paramètres avancés** Dans les **règles de trafic entrant**, filtrées par **bureau à distance**...à 3 règles

2 :une TCP et l'autre UDP...pour le Bureau à distance

1 pour le contrôle à distance

	Pare-feu Windows avec fonctions avancées	Règles de trafic entrant Filtré par : Bureau à distance			
	🔣 Règles de trafic entrant	Nom	Groupe	Profil	
	🌇 Règles de trafic sortant	Pureau à distance - Mode utilicateur (TCD entrant)	Rureau à distance	Tout	
	Negles de sécurité de connexion	Bureau a distance - Mode utilisateur (TCP entrant)	Bureau a distance	Tout	
>	🛃 Analyse	Bureau a distance - Mode utilisateur (ODP entrant)	Bureau a distance	Tout	
		W Bureau à distance - Contrôle à distance (TCP-In)	Bureau à distance	lout	



On voit que le port **TCP-3389** est concerné

Et depuis la version RDP 8 UDP-3389

Propriétés de : Bureau à d	listance (TCP-Ent	trée)		×
Protocoles et ports Général	Étendue Programmes et ser	Avancé rvices	Utilisateurs Ordinateurs	
i s'agit d'une n sont pas modifi	ègle prédéfinie dont ables.	certaines propriét	és ne	
General Nom : Bureau à distance (TCP-Entrée)				
Description : Règle de trafic pour autoriser l	entrant pour le serv e trafic RDP. [TCP 3	ice Bureau à dista 3389]	ince	
,				

Modification Port 3389 du Bureau à Distance

Une machine classique écoute sur TCP 3389 et UDP 3389

C:\User	s\Administrateur>net	stat -a		
Connexi	ons actives			
Proto TCP TCP TCP	Adresse locale 0.0.0.0:135 0.0.0.0:445 0.0.0.0:3389	Adresse distante travail-10:0 travail-10:0 travail-10:0	État LISTENING LISTENING LISTENING	
TCP	0.0.0.0:5357	travail-10:0	LISTENING	
UDP	0.0.0.0:123	* : *		
UDP	0.0.0.0:3389	* *		
UDP	0.0.0.0:3702	* *		
UDP	0.0.0.0:3702	* *		

Le Bureau à Distance port **TCP 3389** par défaut est modifiable via la base de registre dans la Clé HKLMACHINE\System\CurrentControlSet\Control\TerminalServer WinStation\RDp-Tcp\PortNumber



et on peut spécifier un autre N° de port pour accéder au bureau à distance qui écouterais sur un n° de port non configuré par défaut

dans l'exemple ici 6809

Modifier la valeur DWORD 32 bits				
Nom de la valeur :				
PortNumber				
Données de la valeur :	Base			
6809	O Hexadécimale			
	Oécimale			

N.B: le re démarrage du système est obligatoire

Il faut créer une règle spécifique **RDP perso** dans le Pare-feu ...



Pare-feu Windows av	ec fonctions Règles de trafic			
Kègles de trafic es Règles de trafic so Règles de sécurité	ortant Nouvelle règle te a type P	ort	Port Règle qui cont	trôle les connexions d'un port TCP ou UDP.
	Cette règle s'applique t-elle à TCP ou UDP ?)		
	• TCP			
	○ UDP			
	Cette rèale s'applique t-elle à tous les ports lo	ocaux ou à des	ports locaux spécifiq	
	C.T. 1			
	lous les ports locaux			
	Ports locaux spécifiques :	[6809] European 2		
		Exemple : 8	0, 443, 0000-0010	

donnant

Règles de trafic entrant	Propriétés de : RDP perso]
Nom	Général	Programmes et se	rvices	Ordinateurs
🕑 RDP perso	Protocoles et ports	Étendue	Avancé	Utilisateurs
Accès réseau COM + (DCOI Administration à distance C Administration à distance (Règle de pare-feu pour l'ac Règle de pare-feu pour l'ac Règle de pare-feu pour l'ac	Protocoles et ports	tocole : TCP	6 🚎	
Règle de pare-feu pour l'ac O Découverte d'homologue d Extraction du contenu de E	Port local :	Forts sp 6809 Exemple	ecifiques : 80, 443, 5000-3	5010

Pour y accéder depuis un client, il faut ajouter : 'deux-points' et le n° de port à utiliser, comme dans ou

😸 Connexion Bureau à distance		퉣 Connexion Bureau à distance	- • •
Remote Desktop Connection			
Ordinateur : srv-domaine:6809	-	Ordinateur : 192.168.1.222:6809	•



SERVEUR RDS ET DOMAINE

Schéma Configuration RDS

Une installation de base RDS comporte au minimum les machines suivantes en domaine...1 serveur dédié minimum **RDS**



Schéma Configuration avec Gateway RDS

Ce mode ne fonctionne qu'avec 2 serveurs dédiés minimum RDS et Gateway



N.B: si on a un nom de domaine posé sur l'adresse IP, il est plus simple que le nom de domaine externe public soit identique à celui du domaine interne local...(cabare-intra.net)



GROUPE DE SERVEUR 2012

Groupe de Serveur

Il peut être commode depuis un serveur de construire dans l'interface de gestion de serveur une notion de **Groupe de**

Dans **Gérer**

Serveur

on demande **Créer un Groupe de serveur** qui permettra d'avoir accès aux consoles et on outils de supervisions de tous les serveurs du groupe



Il faut donner un nom de groupe, ici formation

	/		
a	Créer un groupe de s	serveurs	_ D X
Nom du groupe de serveur	s formation		
DNS	Importer		
Pool de serveurs	Active Directory	Sélectionné	
Emplacement : Système d'exploitation : Tr Nom (CN) : N	i form	Ordinateur FORM.EDU (2) dc-form rds-form	
Nom Système dc-form Window rds-form Window gtw-form Window	e d'exploitation Is Server 2012 R2 Standard Is Server 2012 R2 Standard Is Server 2012 R2 Standard		

Et demande d'ajouter par exemple les 2 serveurs de notre domaine

Ces serveurs apparaîtront accessibles dans notre gestionnaire de serveur via un nouvel icone de **Groupe**

Gestionnaire de serveur • formation				
Tableau de bord		SERVEUR Tous les ser	S rveurs 2 au tot	al
 Serveur local Tous les serveurs 		Filtrer		<u>م</u>
AD DS AD NS		Nom du serveur	Adresse IPv4	Facilité de gest
formation		RDS-FORM	192.168.1.200	En ligne - Com En ligne - Com
Services de fichiers et d >				5 1



Préconisations :

Les règles suivantes sont à suivre scrupuleusement

- Même si une nouveauté 2012 consiste à rendre possible l'installation des services RD Remote Desktop sur un Contrôleur de Domaine il est peu conseillé de le faire car la sécurité sur un CD est spéciale... (très renforcée)
- Toujours Installer les services sur un serveur déjà membre du domaine. (ne pas faire l'adhésion au domaine après l'ajout des services...)
- Ne jamais installer les applications Avant l'installation du rôle RD sur le serveur 2012, mais toujours Après...
- Ne pas oublier d'installer le serveur de licence... (120 jours pour l'activer auprès de microsoft, puis 90 jours pour installer les CALS sur le serveur...)
- S'il faut gérer des Certificats (pour les Web Service...), le faire Avant d'installer les applications

Si on veut utiliser des fonctions graphiques et/ou multimédia, il faut utiliser les derniers clients RDP

Par défaut, 2 comptes peuvent accéder aux services RD (on a droit à 2 sessions), si on utilise le même compte, la session précédente sera fermée.

N.B: Montage d'un RD Sur un CD (test, maquette...)

du fait de la sécurité renforcée sur le CD, par exemple un utilisateur ne pouvant pas ouvrir de session sur un CD... il ne pourra pas ouvrir de session RD non plus...

Il faudra créer une GPO avec dans

Ordinateur /Stratégies Locales/ Attributions Droits utilisateurs

au minimum les 2 valeurs suivantes

📓 Autoriser l'ouverture de session par les services Bureau à distance

🐻 Permettre l'ouverture d'une session locale

Présentation des Rôles et Services de Rôle Remote Desktop:

5 rôles et services principaux existent

- RDSHRemote Desktop Session hosthôte bureau à distanceRDWARemote Desktop Web Accesportail WebRDLSRemote Desktop Licensing servergestionnaire de licenceRDCBRemote Desktop Connection Brokerservice BrokerRDGRemote Desktop Gatewaypasserelle (*)
 - (*) rôle optionnel
- http://www.cabare.net Page 21 - Michel Cabaré -



RDSH	Remote Desktop Session host	hôte bureau à distance		
	Héberge et accepte plusieurs sessions les applications, et les remoteapps	simultanées, on y installe		
	Nécessite 2 partitions 1 pour l'oS et 1 pour les applications			
	6 Giga Ram 4 cpu			
RDWA	Service de rôle RD Web Acces	portail Web		
	Permet la publication d'un portail pour distance et aux remoteapp	r accéder aux bureaux à		
	4 Giga Ram 4 cpu			
RDLS	Service de rôle RD Licensing server	gestionnaire de licence		
	Gère les licences RDS			
	2 Giga Ram 2 cpu			
RDCB	Service de rôle RD Connection Broker (obligatoire depuis 2012)	service Broker		
	Gèle la connexion et la répartition de charge			
	Ne peut pas s'installer sur un serveur ave	ec une AD		
	6 Giga Ram 4 cpu			
RDG	Service de rôle RD Gateway	passerelle		
	Permet un accès via https 443			
	4 Giga Ram 4 cpu			

Une installation de base RDS comporte au minimum les machines suivantes avec les rôles (ou services de rôle) suivants en domaine...



N.B: il faut absolument installer un Broker depuis la version 2012

ne pas installer le Remote Desktop Connection Broker, c'est ne pas utiliser RDS



Assistant Déploiement infrastructure RDS

Sur un serveur SRV-RDS1, membre du domaine... on se connecte en tant qu'administrateur du Domaine, et on demande via le **gestionnaire de Serveur** d'ajouter un rôle .

On choisit l'assistant Installation des services Bureau à distance

b	Assistant Ajout de rôles et de fonctionnalités		
Sélectionner le ty	pe d'installation	SERVEUR DE DESTINATION Aucun serveur n'est sélectionné.	
Avant de commencer Type d'installation	Sélectionnez le type d'installation. Vous pouvez installer des n ordinateur physique ou virtuel en fonctionnement, ou sur un d	ôles et des fonctionnalités sur un disque dur virtuel hors connexion.	
Type de déploiement	 Installation basée sur un rôle ou une fonctionnalité Configurez un serveur unique en ajoutant des rôles, des se 	rvices de rôle et des fonctionnalités.	
Scénario de déploiement Services de rôle	Installation des services Bureau à distance Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) po		
Service Broker pour les c	déployer des bureaux basés sur des ordinateurs virtuels ou	sur des sessions.	

qui propose 2 solutions :

Déploiement standard : ventilation possible sur plusieurs serveurs Déploiement Rapide : ventilation sur un seul serveur unique

Assistant Déploiement rapide - 1 serveur

On va choisir déploiement rapide, (afin de tout mettre sur le même serveur)



On choisit Le bureau **Déploiement basé sur une session** qui correspondent à la notion de **bureau distant** et de **remote apps** (sinon on fait des VDI...)

B	Assistant Ajout de rôles et de fonctionnalités
Sélectionner le so	serveur de déploiement serveur de déploiement démarrage rapide sélectionné
Avant de commencer Type d'installation Type de déploiement	Les services Bureau à distance peuvent être configurés pour permettre aux utilisateurs de se connecter à des bureaux virtuels, à des programmes RemoteApp et à des bureaux basés sur une session. O Déploiement de bureaux basés sur un ordinateur virtuel
Scénario de déploiement Sélection un serveur	Le déploiement de bureaux basés sur un ordinateur virtuel permet aux utilisateurs de se connecter à des collections de bureaux virtuels incluant des programmes RemoteApp et des bureaux virtuels publiés.
Confirmation Terminé	Déploiement de bureaux basés sur une session Le déploiement de bureaux basés sur une session permet aux utilisateurs de se connecter à des collections de sessions incluant des programmes RemoteApp et des bureaux basés sur une session.



C'est forcément le serveur sur lequel on se trouve....

à	Assistant Ajout de rôles et de fonctionnalités	x
Sélectionner un se	SERVEUR DE DESTINATION Démarrage rapide sélectionné	
Avant de commencer Type d'installation Type de déploiement	Le démarrage rapide installera le service Broker pour les connexions Bureau à distance, le service Accès Web des services Bureau à distance et le service de rôle Serveur hôte de session Bureau à distance sur l même serveur.	e
Scénario de déploiement	Pool de serveurs Sélectionné	
Sélection un serveur Confirmation	Filtre : Ordinateur]
Terminé	Nom Adresse IP Système c gtw-form.form.edu 192.168.1.202 rds-form.form.edu 192.168.1.201 dc-form.form.edu 192.168.1.200 idc-form.form.edu 100.100.100.100.100.100.100.100.100.100	
	< Précédent Suivant > Déployer Annuler	

On confirme et on déploie

a	Assistant Ajout de rôles et de fonctionnalités
Confirmer les sélé	ections serveur de destination rds-form.form.edu
Avant de commencer Type d'installation Type de déploiement Scénario de déploiement Sélection un serveur Confirmation Terminé	Pour terminer l'installation, les serveurs de destination doivent redémarrer. Les services de rôle suivants seront installés sur le serveur nommé rds-form.form.edu. Service Broker pour les connexions Bureau à distance Accès Bureau à distance par le Web Serveur hôte de session Bureau à distance Le serveur va être redémarré après l'installation des services de rôle. Le groupe de sécurité Utilisateurs du domaine sera ajouté au groupe Utilisateurs du Bureau à distance sur le serveur.
•	Redémarrer automatiquement le serveur de destination si nécessaire
	< Précédent Suivant > Déployer Annuler

Il faut cocher pour pouvoir demander Déployer

Et l'installation se déclenche

2	Assistant Ajout de rôle	s et de fonctionnalités	
Afficher la progre	ssion		SERVEUR DE DESTINATIOI rds-form.form.ed
Avant de commencer	Le scénario de déploiement des s	ervices Bureau à distance est en cours d	'installation.
Type d'installation	Serveur	État d'avancement	État
Type de déploiement	Services de rôle des services Bu	ıreau à distance	
Scénario de déploiement	rds-form.form.edu		En cours



RDS 2012 R2 – accès intranet
– SYS 32 – Cours TP - ver 1.3 -http://www.cabare.net
- Michel Cabaré -

Après un redémarrage on doit obtenir

A	Assistant Ajout de rôles	s et de fonctionnalités	_ D X
Afficher la prog	gression		SERVEUR DE DESTINATION Démarrage rapide sélectionné
Terminé	Le scénario de déploiement des se	rvices Bureau à distance est en cours d'ir	nstallation.
	Serveur	État d'avancement	État
	Services de rôle des services Bu rds-form.form.edu	reau à distance	lussi
	Collection de sessions rds-form.form.edu	Ré	iussi
	Programmes RemoteApp rds-form.form.edu	Ré	iussi

Gestionnaire de Serveur - Services Bureau à distance

Dans le gestionnaire de serveur les Services bureau à distance apparaissent

Gestionnaire o	le serveur ∙ Tab	leau de bord
🗰 Tableau de bord	BIENVENUE DANS G	STIONNAIRE DE SERVEUR
Serveur local		
Tous les serveurs		1 Configurer o
IIS IIS	DÉMARRAGE	Configurer e
Ø Services Bureau à distance ▷	RAPIDE	
Services de fichiers et de stockage Þ		2 Ajouter des

Donnant accès à la nouvelle interface de gestion

Gestionnaire c	de serveur • S	ervices Bureau à distance + Vue d'ensemble		
Vue d'ensemble	PRISE EN MAIN DE	ES SERVICES BUREAU À DISTANCE		
Serveurs Collections QuickSessionCollection	DÉMANDACE	Configurer un déploiement p	our les services Burea	u à distance
QuickSessionCollection DéMARAGE RAPIDE EN SAVOIR PLIS		Deploiement de bureaux basés sur un ordinateur virtuel 2 Ajouter des serveurs hôtes de virtualisation des services Burea 3 Créer des collections de bureaux virtuels	 Déploiement de bureaux basés sur une session Ajouter des serveurs hôtes de session Bureau à distance Créer des collections de sessions 	
	Serveur du ser Géré comme : FORM Accès Burear	MBLE DU DÉPLOIEMENT vice Broker pour l Madministrateur Passerelle des service Gestionnaire de licen Service Broker pour l	SERVEURS DE DÉPLOIEMENT Dernière actualisation le 20/05/2016 05 Filtrer Nom de domaine complet du serveur RDS-FORM.FORM.EDU RDS-FORM.FORM.EDU RDS-FORM.FORM.EDU	405:32 Tous les services de rôle des services Bureau à dis P B + P + Service de rôle installé Service Broker pour les connexions Bureau à distance Hôte de session Bureau à distance Accès Web des services Bureau à distance

On peut tester tout de suite l'accès possible à notre serveur RDS via une connexion par le **bureau à distance**



Questions 2008R2 disparues sous 2012 Authentification NLA

Depuis 2012 l'authentification NLA est choisie par défaut

Assistant Ajout de rôles

Question 2008r2

Spécifier une méthode d'authentification pour le service Hôte de session Bureau à distance

×

NLA ou Network Level Authentication	Avant de commencer Rôles de serveurs Services Bureau à distance Services de rôle	L'authentification au niveau du réseau est une nouvelle méthode d'authentification qui améliore la sécurité en fournissant une authentification d'utilisateur plus tôt dans le processus de connexion lorsqu'un client se connecte à un serveur Hôte de session Bureau à distance. Avec l'authentification au niveau du réseau, l'authentification de l'utilisateur intervient avant l'établissement d'une connexion Bureau à distance au serveur Hôte de session Bureau à distance.
nécessite des clients gérant RDP 6.0 minimum	Compatibilité des applications Méthode d'authentification Mode de licence Groupes d'utilisateurs Expérience client	 Spécifiez si l'authentification au niveau du réseau est requise. Exiger l'authentification au niveau du réseau Seuls les ordinateurs qui exécutent une version de Windows et une version du dient Connexion Bureau à distance prenant en charge l'authentification au niveau du réseau peuvent se connecter à ce serveur Hôte de session Bureau à distance. Si vous êtes connecté à distance à ce serveur, vérifiez que votre ordinateur prend en charge l'authentification au niveau du réseau pour permettre une reconnexion à ce serveur.
(Xp Sp2 + install / Seven)	Confirmation État d'avancement Résultats	 Ne nécessite pas l'authentification au niveau du réseau Les ordinateurs qui exécutent une des versions du dient Connexion Bureau à distance peuvent se connecter à ce serveur Hôte de session Bureau à distance. Cette option est moins sécurisée que l'authentification au niveau du réseau car l'authentification intervient plus tard dans le processus de connexion.

Avec RDP <6 quand on se loggait sur un Serveur TSE (2003 par exemple) on arrivait directement sur le bureau TSE2003, PUIS on demandait un login/mot de passe... de fait, on était potentiellement sur le bureau sans être loggué ! (pas mal de failles possibles). Depuis RDP 6 lorsque l'on se loggue sur un serveur RDP avec NLA, la demande d'authentification est incorporée DANS la connexion réseau AVANT d'être sur le bureau. Ce qui est plus sûr...

N.B : si on ne veut ne pas d'authentification RDP, mettre en place SSO

• Si on veut gérer NLA pour le bureau à distance, il suffit de paramétrer son accès via le gestionnaire de Serveur, Serveur local puis Bureau à distance



N.B: Si la case a cocher est inaccessible c'est que l'on à paramétrer le serveur

N'autoriser que la connexion des ordinateurs exécutant le Bureau



http://www.cabare.net Page 26 - Michel Cabaré -

à distance avec authentification NLA (recommandé)

Si on veut gérer NLA pour ses accès distants, on peut gérer soit par l'interface graphique, en modifiant les propriété de la collection de session

→ Gestionnaire de	serveur • Services Bureau à distance • Collections • QuickSessionCollec	tion
Vuo d'ancomblo	PROPRIÉTÉS Propriétés de la collection TÂCHES	🚽 🕈 💡
Serveurs	Type de collection Session Mo	difier les proprié
Collections	Ressources Programmes RemoteApp	
QuickSessionCollection	Groupe d'utilisateurs FORM\Utilisateurs du domaine	
Dans Sécurité		
a	QuickSessionCollection Propriétés	x t
Afficher Général Groupes d'utilisate. Session <u>Sécurité</u> Équilibrage de la c Baramàtres du clio	tout + Configurer les paramètres de sécurité+ Spécifiez les paramètres de sécurité entre le client et les serveurs hôtes de session Bu distance dans la collection de sessions+ Couche de sécurité :+	Jreau à
Disques de profil	Négocier La couche la plus sécurisée prise en charge par le client sera utilisée. Si le protocole S (TLS 1.0) est pris en charge, il sera utilisé. Niveau de chiffrement : Compatible client Toutes les données envoyées entre le client et le serveur sont protégées par un chiffi basé sur la puissance de clé maximale prise en charge par le client. Autoriser les connexions uniquement pour les ordinateurs exécutant les services	SL ;SL rement
	à distance avec authentification au niveau du réseau	bureau

Soit par stratégie gpedit.msc)

Stratégie ordinateur / modèles d'administration / Composants Windows / Services Bureau à distance / hôte de la session Bureau à distance /Sécurité



pour les connexions à distance à l'aide de l'authentification au niveau du réseau

Sécurité

ڬ Sécurité			
Requérir l'authentification		Paramètre	État
utilisateur pour les connexions à		Modèle de certificat d'authentification serveur	Non configuré
distance à l'aide de l'authentificati	ion	Définir le niveau de chiffrement de la connexion client	Non configuré
au niveau du reseau		Toujours demander le mot de passe à la connexion	Non configuré
Si vous désactivez ce paramètre de	~	Requérir des communications RPC sécurisées	Non configuré
niveau du réseau n'est pas		Nécessite l'utilisation d'une couche de sécurité spécifique p	Non configuré
nécessaire pour l'authentification		🖹 Ne pas autoriser les administrateurs locaux à personnaliser l	Non configuré
des utilisateurs avant d'autoriser		Requérir l'authentification utilisateur pour les connexions à	Désactivé
les connexions distantes au			
à distance.			





http://www.cabare.net Page 27 - Michel Cabaré -

Serveur de Licence

les

Bureau

Rien n'est demandé lors de l'installation. on temporise pour l'instant (120 jours de carence) MAIS il faudra installer un serveur de Licence...

d'ailleurs dès les premières connexions on a ce genre de message qui peut apparaitre

🥼 Le mode de licence Bureau à distance n'est pas configuré. 🔌 X Les services BD vont s'arrêter dans 119 jours. Sur le serveur Broker pour connexions BD, utilisez le Gestionnaire de serveur pour spécifier le mode de licence des services BD et le serveur de licences.

L'installation d'un serveur

de Licence est une des premières choses à faire.

Qui peut utiliser les services RDS

Il s'agit d'indiquer un groupe d'Utilisateurs du domaine dans le groupe local du serveur RDSH nommé Utilisateurs du Bureau à distance.

Assistant Ajout de rôles × Sélectionner les groupes d'utilisateurs autorisés à accéder à ce serveur Hôte de session **Question 2008r2** Bureau à distance Qui peut utiliser Avant de commencer Ajoutez les utilisateurs ou les groupes d'utilisateurs qui peuvent se connecter à ce serveur Hôte de session Bureau à distance. Ces utilisateurs et groupes d'utilisateurs seront ajoutés au groupe Utilisateurs du Bureau à services Rôles de serveurs distance. Le groupe Administrateurs est ajouté par défaut et ne peut pas être supprimé. à Services Bureau à distance distance Utilisateurs ou groupes d'utilisateurs : Services de rôle Compatibilité des applications Administrateurs Ajouter Méthode d'authentification 好 Mode de licence Groupes d'utilisateurs

Sous 2012r2 le groupe des Utilisateurs du domaine est ajouté dans le groupe local nommé Utilisateurs du Bureau à distance en plus des administrateurs, qui eux ont un accès d'office (même s'ils ne paraissent pas !)



N.B: pour plus de clarté il vaudrait mieux créer un groupe Spécifique,



Par exemple avec un nom explicite, genre Utilisateurs-RDS...

	Nouve	l objet - Groupe	X	
	🥵 Créer dans : form.e	du/formation		
	Nom du groupe : Utilisateurs-RDS		-	
	Nom de groupe (antérieur à Windo Utilisateurs-RDS	ws 2000) :		
Contenant nos utilisateurs	Étendue du groupe O Domaine local I Globale	Type de groupe Sécurité Distribution		
	-			

Nom	Туре
& bob	Utilisateur
& Utilisateurs-RDS	Groupe de sécurité - Global

Et ensuite mettre ce groupe <u>à la place</u> de tous les utilisateurs du domaine dans le **groupe local** du serveur **RDSH** nommé **Utilisateurs du Bureau à distance**

et enfin on peut supprimer

Propriétés	de : Utilisateurs du Bureau à distance 🛛 📍 🗙							
Général								
Utilisateurs du Bureau à distance								
Description : Les membres de ce groupe disposent des droits nécessaires pour ouvrir une session à distance								
Membres :								

Experience Utilisateur

Pourquoi ajouter ces fonctions **Experience Utilisateur** sur le serveur RDS ? et bien lorsqu'un utilisateur RDP se loggue, il a un bureau reproduit à partir de celui du serveur Hôte !



Ce qui correspondait à la fonction Experience Utilisateur sur le serveur 2008r2



Donc si on veut que l'utilisateur puisse avoir un bureau type Windows 8.1 (Paramètres du PC - Outil de Capture d'écran - Nettoyage de disque - Table des caractères - Lecteur Windows Media - Programmes par défaut - Windows Store...) il faut installer la fonctionnalité Experience Utilisateur sur le serveur hôte RDS 2012r2.

Sélectionner le ty	SERVEUR DE DESTINATION rds-form.form.edu	
Avant de commencer	Sélectionnez le type d'installation. Vous pouvez installer des rôles et ordinateur physique ou virtuel en fonctionnement ou sur un disque	des fonctionnalités sur un dur virtuel hors connexion
Type d'installation	orannateur physique ou virtuer en fonetionnement, ou sur un usque	dur virtuer nors connexion.
Sélection du serveur	Installation basée sur un rôle ou une fonctionnalité Configurez un serveur unique en aioutant des rôles, des services (de rôle et des fonctionnalités.
Rôles de serveurs		
Fonctionnalités	Installation des services Bureau à distance	
Confirmation	Installez les services de role necessaires à l'infrastructure VDI (Virt déployer des bureaux basés sur des ordinateurs virtuels ou sur de	ual Desktop Infrastructure) pour es sessions.

Il faut juste dans les Fonctionnalités demander Experience Utilisateur dans Interfaces et infrastructure

b		Assistant Ajout de rôles et de fonctionnalités								
Séle	Sélectionner des fonctionnalités									
Ava	nt de commencer	Sélectionnez une ou plusieurs fonctionnalités à installer sur le se	rveur sélectionné.							
Тур	e d'installation	Fonctionnalités	Description							
Séle	ection du serveur	Gestion du stockage Windows base sur des norme	L'Expérience utilisateur comprend							
Rôle	es de serveurs	IFilter TIFF Windows	les fonctionnalités de Windows 8.1, dont Windows Search, qui vous							
Fon	ctionnalités	IIS Hostable Web Core	permet de lancer une recherche sur							
Con	nfirmation	▲ Interfaces utilisateur et infrastructure (2 sur 3 insta	votre périphérique et sur Internet depuis un même emplacement. Pour							
Rés	ultats	 Outlis et infrastructure de gestion graphique (i Expérience utilisateur Shell graphique du serveur (Installé) Kit d'administration du Gestionnaire des connexio Media Foundation (Installé) 	en savoir plus sur l'Expérience utilisateur, notamment sur la désactivation des résultats Web dans la Recherche Windows, consultez http://go.microsoft.com/ fwlink/?Linkld=390729							
_'instal	lation se lance									
	a	Assistant Ajout de rôles et de fonctionnali	tés 📃 🗖 🗙							
	Progression	de l'installation	SERVEUR DE DESTINATION rds-form.form.edu							

	Continue d'anna et de concercience de l'éculture monuration
	Evnérience utilisateur
Fonctionnalités	Interfaces utilisateur et infrastructure
	Installation démarrée sur rds-form.form.edu
Sélection du serveur	
Type d'installation	i Installation de fonctionnalité
Avant de commencer	Afficher la progression de l'installation

Et nécessitera un redémarrage du serveur !

N.B: L'installation de la fonctionnalité **Expérience utilisateur** n'active pas automatiquement les fonctionnalités qu'elle-même installe. À l'issue de l'installation, vous devez activer manuellement toutes les fonctionnalités qui requièrent des modifications de configuration



TESTER LE BUREAU A DISTANCE

1° connexion Bureau à Distance

On peut utiliser une **adresse Ip** (si non membre d'un domaine) ou un nom machine FQDN (mieux)





N.B: Pour éviter que à chaque lancement du bureau à distance,, l'authentification soit à re-saisir, on peut demander dans les options de mémoriser... cela enregistrera le login de connexion dans les **options** onglet **Général**





Gérer les connexions en Cours (service bureau à distance)

Depuis le poste **Serveur 2012R2** si les **Service bureau à distance** sont installés (et uniquement si) on peut visualiser les connexions distantes en cours de session

Il faut dans le gestionnaire de Serveur, se placer sur les Services bureau à distance, puis Collections

\mathbf{E}	●	aire de serveur • Services Bureau à distance • Collections •
	Vue d'ensemble	COLLECTIONS Dernière actualisation le 19/05/2016 08:00:46 Toutes les collections 1 au total
i i	Serveurs	
Ī	Collections	
6	QuickSessionCo	Nom Type Taille Type de ressource État
⊗ ⊳		QuickSessionCollection Session 1 Programmes RemoteApp

N.B : on verra ultérieurement les collections

Sur la partie basse à droite on devrait afficher une zone nommée Connexions

SERVEURS HÔT Dernière actualisat	FES tion le 19/05/2016 08:00:46 Tous le	s serve TÂCHE	s 🔻	CONNEXIONS Dernière actualisation le	19/05/2016 11:23:02 Toutes les con [TÂCHES 🔻
Filtrer		• • •	۲	Filtrer	(ii) 	• •
Nom du serveur	Туре	Bureaux virtuels	Autor	Nom de la collection	Nom de domaine complet du serveur	Utilisateur
RDS-FORM	Hôte de session Bureau à distance	N/A	Vrai	QuickSessionCollection	rds-form.form.edu	FORM\Admin

Affichant

CONNEXIONS Dernière actualisation le 19/05/2016 12:12:52 Toutes les connexions 2 au total								
Filtrer	Q							۲
Nom de la collection	Nom de domaine	Utilisateur	État de la session	Bureau virtuel	Heure d'ouverture de session	Heure de déconnexion	Durée d'inactivité	
QuickSessionCollection	rds-form.form.edu	FORM\Administrateur	Actif	-	19/05/2016 07:58:00	-	-	
QuickSessionCollection	rds-form.form.edu	FORM\bob	Déconnecté	-	19/05/2016 12:00:27	19/05/2016 12:03:48	00:09:04.1970000	

Un clic – droit sur la connexion **rdp** voulue permet de faire l'essentiel...

CONNEXIONS Dernière actualisation le 1	19/05/2016 12:12:52	Toutes les co	onnexior	ns 2	au total
Filtrer	Q		•		
Nom de la collection	Nom de domaine	Utilisateu	r		État de la session
QuickSessionCollection	rds-form.form.edu	FORM\Ad	ministra	teur	Actif
QuickSessionCollection	rds-form.form.edu	FORM\bo	b	Déco Envo Clich	onnexion oyer un message né instantané
				Form	ar la cassion



On voit très clairement la visualisation d'un utilisateur qui se déconnecte proprement, d'un utilisateur qui ferme brutalement sa session

CONNEXIONS Dernière actualisation le 19/05/2016 13:12:07 Toutes les connexions 2 au total								
Filtrer	م							
Nom de la collection	Nom de domaine	Utilisateur	État de la session	Bureau virtuel	Heure d'ouverture de session			
QuickSessionCollection	rds-form.form.edu	FORM\Administrateur	Actif	-	19/05/2016 07:58:00			
QuickSessionCollection	rds-form.form.edu	FORM\bob	Actif		19/05/2016 12:00:27			

Il se déconnecte brutalement, sa session est toujours « existante »

CONNEXIONS Demière actualisation le 19/05/2016 13:13:20 l'Toutes les connevions 1,2 au total						
Filtrer	٩					
Nom de la collection	Nom de domaine	Utilisateur	État de la session	Bureau virtuel	Heure d'ouverture de session	Heure de déconnexion
QuickSessionCollection	rds-form.form.edu	FORM\Administrateur	Actif	-	19/05/2016 07:58:00	-
QuickSessionCollection	rds-form.form.edu	FORM\bob	Déconnecté	-	19/05/2016 12:00:27	19/05/2016 13:13:13

Il se deconnecte proprement, sa session disparait

CONNEXIONS

Dernière actualisation le 19/05/2016 13:15:16 Toutes les connexions 1 au total							
Filtrer	م						
Nom de la collection	Nom de domaine	Utilisateur	État de la session	Bureau virtuel	Heure d'ouverture de session	Heure de déconnexion	
QuickSessionCollection	rds-form.form.edu	FORM\Administrateur	Actif	-	19/05/2016 07:58:00	-	

Remote Desktop Shadowing

Remise en place avec **2012R2** il est possible de prendre le contrôle d'une session RDP, soit en miroir, soit en contrôle

On se place sur la session à monitorer/prendre, clic droit et on demande Cliché instantané



Tout est dit dans la boite de dialogue qui s'affiche

N.B : si on veut se passer de la demande d'autorisation envoyée par défaut à l'utilisateur, (en décochant la case..) il faut gérer une stratégie pour définir les options voulues





RDS 2012 R2 – accès intranet – SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 33 - Michel Cabaré - il faut faire une stratégie (ou gpedit.msc)

Stratégie ordinateur / modèles d'administration / Composants Windows / Services Bureau à distance / hôte de la session Bureau à distance /Connexions



Et on Active la stratégie Définir les règle de contrôle à distance des sessions utilisateurs des services bureau à distance

Connexions			
Définir les règles pour le contrôle à		Paramètre	État
distance des sessions utilisateur de	s	🖹 Reconnexion automatique	Non configuré
services Bureau à distance		🗈 Autoriser les utilisateurs à se connecter à distance à l'aide de	Non configuré
Madifianta anno 2011 de statégie		🖹 Refuser la déconnexion d'un administrateur connecté à la se	Non configuré
Modifier <u>le parametre de strategre</u>		🖹 Configurer l'intervalle de conservation des connexions	Non configuré
Configuration requise :		🖹 Limiter le nombre de connexions	Non configuré
Windows Server 2008 R2, Windows		🖹 Suspendre la connexion de l'utilisateur pour terminer l'inscri	Non configuré
Server 2008, Windows Server 2003,		Définir les règles pour le contrôle à distance des sessions util	Activé
Windows XP		Sélectionner la détection du réseau sur le serveur	Non configuré

En choisissant un niveau... Ici 3...

Paramètre précéc	lent Paramètre sui	vant		
○ Non configuré	Commentaire :			
 Activé 				
O Désactivé				
	Pris en charge sur :	Windows S Windows 7	ierver 2008 R2, Windows Server 2008, Windows Server 2003, 7, Windows Vista et Windows XP	
Options :			Aide :	
			1. Aucun contrôle à distance autorisé : interdit à un	_

Remote Desktop Shadowing invite de commande

Les options de mstsc sont nombreuses et affichables via mstsc/?

Une autre commande sera nécessaire, la commande **query** permet de récupérer l'ID d'une session RDP..

Query session /server :192.168.1.201

C:\Users\Administr SESSION	ateur.FORM>query UTILISATEUR	session /ser ID	ver:192.1 ÉTAT	168.1.201 TYPE
services rdp-tcp#27 console 31c5ce94259d4 rdp-tcp	bob Administrateur	0 1 2 65536 65537	Déco Actif Actif Écouter Écouter	

dans l'exemple on prend le contrôle de la session RDP de bob, ID numéro 1

Mstsc /shadow:1 /control /noconsentprompt



Mise en Evidence Remote-FX

Un essai pour mettre en évidence **RemoteFX**... On peut constater qu'une utilisation bureautique, la consommation de bande passante est quasi-nulle !)



Mais même avec une vidéo HQ... cela reste raisonnable 10Mb/s

On va chercher sur le serveur RDS une video HQ de 120Mo que l'on a placé dans un dossier **video-hd**

🛛 📗 Utilisateurs	^	Nom	Modifié le	Туре	Taille
Utilitaires video-hq		Alexander_Trailer_1080p.wmv	11/10/2004 19:39	Fichier audio/vidé	129 189 Ko
▷ Windows		Thumbs.db	31/08/2013 14:46	Data Base File	8 Ko

Un fois l'experience utilisateur installée, pour avoir Windows Media player





Les Collections RDS 2012 :

une collection RDS, (nouveauté 2012) est un moyen de regrouper des serveurs RDSH en « fermes », séparées les unes des autres...

N.B : Un serveur RDS ne peut faire partie que d'une collection à la fois !

Il existe des collections de session et des collections de Bureaux virtuels VDI, on ne gèrera ici que les collections de session.

Les Collections de session:

Lorsque l'on crée un déploiement rapide sur un seul serveur RDS, l'assistant installe automatiquement une collection de session nommée **QuickSessionCollection**

Avec comme type de ressource Programmes Remote App avec 3 programmes « test » publiés, la calculatrice, paint et wordpad

On visualise cela dans le Gestionnaire de serveur, dans les Services de Bureau à distance, en se plaçant sur Collections

●	aire de serveur • Services Bureau à distance • Collections •
Vue d'ensemble Serveurs Collections	COLLECTIONS Dernière actualisation le 22/05/2016 09:26:45 Toutes les collections 1 au total Filtrer P (III) ~
QuickSessionCo	Nom Type Taille Type de ressource État
	QuickSessionCollection Session 1 Programmes RemoteApp

Si on se place sur		Gestionnaire de serveur	
une collection, ici dans l'exemple la	→ · Collections	QuickSessionCollection	• ©
collection QuickSessionColl ection	Vue d'ensemble Serveurs Collections	PROPRIÉTÉS Propriétés de la collection TÂ Type de collection Session Ressources Programmes RemoteApp	CHES 👻
on peut la paramétrer finement	QuickSessionCollection	Groupe d'utilisateurs FORM\Utilisateurs du domaine PROGRAMMES REMOTEAPP Dernière actualisation le 22/05/2016 09:26:45 Programmes TÂ Filtrer	CHES V
		Nom du programme RemoteApp Alias Visible dans l'Accé Calculatrice Calculatrice Oui Paint Paint Oui	ès Web des
		WordPad WordPad Oui	
pabaré 🔊 RDS 20	12 R2 – accès intranet	http://www.cabare.net Page 36	

– SYS 32 – Cours TP - ver 1.3 -

http://www.cabare.net Page 36 - Michel Cabaré -
Les éléments d'une Collection:

une collection de session RDS, peut héberger 2 types de ressources :

- un Bureau à distance (par défaut) •
- un ou des Programmes RemoteApp •

Par défaut lorsque l'on crée une collection, les ressources installées dessus sont de type bureaux à distance. Si on installe des Programmes RemoteApp (voir chapitre spécifique) alors les bureaux à distances sont automatiquement remplacés par les ressources Remote App



Ce (ces) serveur contient des ressource publiées, soit des RemoteApp (soit un Bureau à distance)



Paramétrages simples d'une Collection:

On se place sur la collection et on demande Taches / Modifier les propriétés

Vue d'ensemble	PROPRIÉTÉS Propriétés de la co	PROPRIÉTÉS Propriétés de la collection		COI Derr
Serveurs	Type de collection	Session	Modifier	les propriétés
Collections	Ressources	Programmes RemoteApp		h
QuickSessionCollection	Groupe d'utilisateurs	FORM\Utilisateurs du domaine		Nc

Général

our défini	r un non _	n Général
Converse divitili		General
Groupes d'utili	sate +	
Session	+	Le nom de la collection de sessions s'affiche pour les utilisateurs lorsqu'ils ouvrent une
Sécurité	+	session d'accès Web des services Bureau à distance.
Équilibrage de la c + Paramètres du clie +		Nom :
		formation RDS 2012
Disques de pro	fil +	Description (facultative) :

Groupe d'utilisateurs

Plutôt de laisser les utilisateurs du domaine préférer travailler avec des groupes plus précis

Général + Groupes d'utilisate		Spécifier des groupes d'utilisateurs				
Session + Sécurité + Équilibrage de la c + Paramètres du clie + Disques de profil +		Ajoutez les groupes d'utilisateurs à associer à cette collection de sessions. Les utilisateurs membres de ces groupes peuvent se connecter aux serveurs Hôte de session Bureau à distance membres de cette collection et peuvent accéder aux programmes RemoteApp publiés.				
					Groupes d'utilisateurs :	
					FORM\Utilisateurs-RDS Ajouter	
		FORM\Admins du domaine	_			
		Supprime	r			

Session

Selon les contraintes, un compromis pourrait être le suivant Général

Général	+	Configurer les paramètres de session	on
Groupes d'utilisate	+		
Session	-	Définissez les paramètres de délai d'expiration et de	reconnexion pour le serveu
Sécurité	+	session Bureau a distance pour la collection de sess	ions.
Équilibrage de la c	+	Mettre fin à une session déconnectée :	Jamais
Paramètres du clie	+	Limite de la session active :	12 heures
Disques de profil	+	Limite de session inactive :	5 minutes
		Lorsqu'une limite de session est atteinte ou qu'une Se déconnecter de la session Activer la reconnexion automatique	connexion est interrompue :

O Mettre fin à la session

Paramètres de dossier temporaire :

- Supprimer les dossiers temporaires en quittant
- \checkmark Utiliser des dossiers temporaires par session



serveur hôte de

-

-

•

GESTIONNAIRE DE LICENCES

Importance Du Gestionnaire :

Le **Gestionnaire de Licence**, est un Serveur indispensable. Il peut être installé sur un DC, mais peut aussi être installé sur un serveur dédié (...)

S'il "tombe", on n'a <u>plus aucune connexion RDS</u> possibles. Comme il en se redonde pas, (licences uniques...) soit

- On se débrouille pour qu'il soit facilement "restaurable" en cas de crash (genre VM et serveur dédié...)
- On peut l'installer sur le DC qui héberge les 5 rôles FSMO, car la restauration de ce DC restaurera aussi notre serveur de licence. MAIS on ne l'installe pas sur un DC secondaire (comme on ne restaure jamais la VM d'un DC secondaire) on devrait sinon effectuer une restauration non autoritaire de l'AD qui incorpore le gestionnaire de licence
- On en met en place 2, ayant chacun de 50% des licences à distribuer

N.B: si un serveur de licence est placé sur un DC, la sauvegarde et le restauration de l' **AD system state** incorpore le **serveur de licence (** donc en effectuant une **restauration non autoritaire du système state** on récupère une sauvegarde du serveur de licence)

Le gestionnaire de licence est donc une machine "critique".

- On dispose de **120 jours** de grâce lorsque l'on installe un serveur RDS, avant que l'absence de serveur de licence ne bloque tout.
- Puis on encore **90 Jours** pour installer les premières CAL sur le serveur...

3 types de Licences RDS CAL:

On peut avoir soit un gestionnaire de licences VDI soit un gestionnaire de licences RDS. Nous on a besoins d'une gestionnaire RDS gérant des RDS CALS Remote Desktop Services Client Access License (Ce qui auparavant se nommait TS CAL Terminal Services Client Access Licence)

Il existe désormais 3 types de licences RDS CAL

• Par **Périphérique** = authentification par **UC/Poste**

On peut donc connecter un nombre illimité d'utilisateurs mais depuis toujours la même machine

• Par Utilisateur = authentification par Login/Mdp

On peut donc connecter un seul utilisateur mais depuis n'importe quelle machine

 Dite External Connector (nouveauté 2012) pour connecter un nombre illimité utilisateur depuis des machines externes (son prix est d'environ 100x la Cal par utilisateur, en dessous de ce barème, il vaut mieux utiliser des CAL utilisateurs)

N.B: au niveau du serveur RDS, un seul choix sera possible, soit Périphérique, soit Utilisateur. Si on veut proposer les 2 Solutions il faudra 2 Serveurs RDS

N.B: au niveau du **serveur de Licence** les types de CAL, **Périphérique** et **Utilisateur**, sont mixables



Ajour service de Rôle Gestionnaire de licence:

Le gestionnaire de Licence, est une fonctionnalité de rôle, par conséquent le rôle n'a pas besoin d'être installé pour que la fonction le soit...

En d'autres termes, cela veut dire que l'on peut placer le serveur de licence

- sur un serveur dédié
- sur un (ou le) serveur RDSH
- sur un (ou le) **CD**. Ce qui permettrait de sauvegarder le serveur de licence RDS avec le CD

il va falloir maintenant installer un serveur de licence, et vérifier que ce serveur de licence soit bien référencée dans notre déploiement RDS..

Dans le **gestionnaire de serveur** sur lequel on a installé le rôle RDS on demande les **Services bureau à distance**

La manière la plus intuitive d'ajouter un serveur de licence c'est de cliquer dans la **Vue d'ensemble du déploiement** sur **Gestionnaire de licence**



On peut aussi demander dans les Serveurs de Déploiement d'Ajouter des serveurs du gestionnaire de licences...



On choisit le serveur voulut (* si 1 seul serveur paraît voir N.B. plus bas)

🚡 Ajouter	Gestionnaire de licences	des services Bu	ireau à distai	nce serveurs	_ D X
Sélectionner un se	erveur				
Sélection un serveur Confirmation Résultats	Cet Assistant vous permet o serveurs au déploiement. S Gestionnaire de licences de	d'ajouter Gestionna électionnez les serv s services Bureau à	ire de licences o eurs sur lesque distance.	des services Bureau à ls installer le rôle de s	distance ervice
	Pool de serveurs Filtre :			Sélectionné Ordinateur	
	Nom rds-form.form.edu	Adresse IP 192.168.1.201 192.168.1.200	Systèm	•	
	dc-form.form.edu	192.168.1.200		▶	



RDS 2012 R2 – accès intranet - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 40 - Michel Cabaré -

🚡 Ajouter	er Gestionnaire de licences des services Bureau à distance serveurs 📃 🗕 🗖 🗙					
Afficher la progre	Afficher la progression					
Sélection un serveur Le service de rôle est en cours d'installation sur les serveurs suivants.						
Confirmation	Confirmation Serveur État d'avancement État					
Résultats	Service de rôle Gestionnaire de licences des services Bureau à distance dc-form.form.edu					

On peut vérifier que le gestionnaire de licence est bien installé, dans la Vue d'ensemble du déploiement le Gestionnaire de licence est ok

VUE D'ENSEMBLE DU DÉI Serveur du service Broker pou	PLOIEMENT r les connexions Bureau à distance :	rds-form.edu TÂCHES 💌
Géré comme : FORM\Administrateu	r	
	•	
Accès Bureau à dista	Passerelle des service	Gestionnaire de licen
	Service Broker pour I	

dans les Serveurs de Déploiement le Gestionnaire de licence est listé

SERVEURS DE DÉPLOIEMENT Dernière actualisation le 20/05/2016 07:05:25 Tous les services de rôle des services Bureau à distance 4 au total				
Filtrer				
Nom de domaine complet du serveur	Service de rôle installé			
dc-form.form.edu	Gestionnaire de licences des services Bureau à distance			
RDS-FORM.FORM.EDU	Service Broker pour les connexions Bureau à distance			
RDS-FORM.FORM.EDU	Hôte de session Bureau à distance			
RDS-FORM.FORM.EDU	Accès Web des services Bureau à distance			

N.B : Si on regarde sur le serveur form-DC le gestionnaire de licence a été installé, et uniquement lui.

b	Assistant Ajout de rôles et de fonctionnalités	_ □ ×
Sélectionner des I	ôles de serveurs	SERVEUR DE DESTINATION dc-form.form.edu
Avant de commencer	Sélectionnez un ou plusieurs rôles à installer sur le serveur sélec	tionné.
Type d'installation	Rôles	Description
Sélection du serveur	Services AD RMS (Active Directory Rights Manage	Les services Bureau à distance
Rôles de serveurs	Services Ab Kivis (Active Directory Highls Manage	permettent aux utilisateurs
Fonctionnalités	Accès Bureau à distance par le Web	d acceder aux bureaux virtueis, aux bureaux basés sur une session et aux
Confirmation	Gestionnaire de licences des services Bureau à	programmes RemoteApp. Utilisez
Résultats	Hôte de session Bureau à distance	l'installation des services Bureau à distance pour configurer un
	Hôte de virtualisation des services Bureau à dis	déploiement de bureaux basés sur
	Passerelle des services Bureau à distance	un ordinateur virtuel ou sur une
	Service Broker pour les connexions Bureau à di	session.



NB : si un seul serveur apparaît dans la liste

🖹 Ajo	uter Gestionnaire de licen	ices des services Bureau à distance serveurs 📃 🗕 🗖 🗙		
Sélectionner u	n serveur			
Sélection un serveur Confirmation	Cet Assistant vous perr serveurs au déploieme Gestionnaire de licence	met d'ajouter Gestionnaire de licences des services Bureau à distance nt. Sélectionnez les serveurs sur lesquels installer le rôle de service es des services Bureau à distance.		
	Pool de serveurs	Pool de serveurs Sélectionné		
	Filtre :	Ordinateur		
	Nom	Adresse IP Systèm		
	rds-form.form.edu	192.168.1.201		

c'est qu'il faut au niveau du **Gestionnaire de Serveur** ajouter d'autres Serveur que celui sur lequel on est!

donc Ajouter d'autres serveurs à gérer

€ Gestionnaire de serveur → Tableau de bord			
🎹 Tableau de bord	BIENVENUE DANS GESTIONNAIRE DE SERVEUR		
Serveur local Tous les serveurs	1 Configurer ce serveur local		
Image: Services Bureau à distance ▷ Image: Services de fichiers et de stockage ▷	Ajouter des rôles et des fonctionnalités		
	NOUVEAUTÉS 4 Créer un groupe de serveurs		
	EN SAVOIR PLUS		
	Rôles et groupes de serveurs Rôles : 3 Groupes de serveurs : 1 Nombre total de serveurs : 1		

Et on ajoute les serveurs voulus

i	Ajouter des serve	eurs 📃 🗖 🗙
	Active Directory DNS Importer Emplacement : importer form > importer Système d'exploitation : Tous importer Nom (CN) : Nom ou début du nom Rechercher maintenant	Sélectionné Ordinateur
	Nom Système d'exploitation dc-form Windows Server 2012 R2 Datacenter rds-form Windows Server 2012 R2 Standard	



Paramétrage du Gestionnaire de licence:

N.B : cette action est à faire <u>depuis la machine</u> ou l'on a installé le **Rôle** gestionnaire de licence.

Il faut effectuer 2 paramétrages pour notre serveur de licences :

- Activer le serveur de licence
- Ajout du serveur dans un groupe de Sécurité nommé Serveur de licence des services terminal Server

Le gestionnaire de Licence a été installé sur un serveur, dans notre exemple **dc-form**, , Si seul ce rôle ai été installé, et donc l'accès à l'interface de gestion disponible via les gestionnaire de serveur n'est même pas opérationnelle,



cela n'a pas d'importance car une console d'administration devient disponible dans les **outils d'administration**, nommée **Gestionnaire de licence des Services bureau à distance.**

鷆 « Out	ils d'administration 🔸 Services Bureau à distance
	Nom
	desktop.ini
ents récer	🚌 Gestionnaire de licences des services Bureau à distance

On la lance

%		Gestionnaire de li	icences des services	Bureau à distance
Action Affichage ?				
Tous les serveurs	Nom	État de l'activation	Étendue de la déco	Configuration
DC-FORM	DC-FORM	Non activé	Domaine	<u>Révision</u>

Activation du Gestionnaire de licences:

Pour déclarer auprès de Microsoft un serveur de licence RDS il faut aller dans le **Gestionnaire de licences des services Bureau à distance**

Le serveur apparaît en rouge... via Clic-droit on demande Activer le Serveur

9				Gestionnaire de licenc	es des services Bureau à distance
Action Affichage ?					
🕀 🙀 Tous les serveurs	Nom	État de l'activation	Étendue de la déco	Configuration	
	SRV-DC1	Non activé	Domaine	<u>Révision</u>	
		Actualiser			
		Revoir la configuration			
		Installer les licences			
		Activer le serveur	•		1
		Avancé	•		

Un assistant se déclanche





Assist	ant Activation du serveur	
F	echerche du serveur Microsoft Clearinghouse	
	Annuler	

Cette partie est importante

celle-ci moins...

Assistant Activation du serveur	Assistant Activation du serveur
Informations sur la société	Informations sur la société
Foumissez les informations requises concernant la société.	Entrez ces informations facultatives.
Entrez votre nom, le nom de votre société et votre pays/région. Ces informations sont nécessaires pour continuer. Prénom : michel Nom de famille : cabaré Société : Formation Cabaré Pays ou région : France v	Adresse de messagerie : contact@cabare.net Unité d'organisation : Formation Adresse de la société : 67 bvd joliot curie Ville : Forntaine Département ou région : isère Code postal : 38600
Le nom et les informations sur la société ne sont utilisés que par Microsoft si vous avez	Si les informations facultatives sont entrées dans cette page, elles ne seront
besoin d'assistance. Le champ Pays/Région est obligatoire pour se conformer aux	utilisées que par les professionnels du support technique Microsoft si vous avez
restrictions d'exportation en vigueur aux Etats-Unis.	besoin d'assistance.

Puis on décoche pour ne pas enchainer tout de suite sur la saisie des licences

Fin de l'Assistant Activation du serveur L'Assistant Activation du serveur est terminé. État : Votre serveur de licences a été activé correctement. Pour installer des licences, cliquez sur Suivant. Pour remettre à plus tard l'installation des licences.	Assistant Activation du serveur	x
désactivez la case à cocher Démarrer l'Assistant Installation de licences, puis cliquez sur Terminer.	Fin de l'Assistant Activation du serveur L'Assistant Activation du serveur est terminé. État : Votre serveur de licences a été activé correctement. Pour installer des licences, cliquez sur Suivant. Pour remettre à plus tard l'installation des licences, désactivez la case à cocher Démarrer l'Assistant Installation de licences, puis cliquez sur Terminer.	

Et notre serveur de licence s'active. Mais avec une icône de warning

9a				Gestionnaire de lic	ences des
Action Affichage ?					
🗉 🛱 Tous les serveurs	Nom	État de l'activation	Étendue de la déco	Configuration	
	SRV-DC1	Activé	Domaine	<u>Révision</u>	

N.B: l'icône attention signifie que notre serveur n'est pas encore inscrit dans le dans le groupe de Sécurité, même s'il est "connu" de notre distribution RDS



http://www.cabare.net Page 44 - Michel Cabaré -

Ajout dans Groupe de Sécurité Serveur de licence des services terminal Server:

Il suffit soit via clic droit de demander Revoir la configuration, soit de cliquer sur la configuration en cours Révision

9				Gestionnaire de lice	ences
Action Affichage ?					
	Nom	État de l'activation	Étendue de la déco	Configuration	
	SRV-DC1	Activé	Domaine	<u>Révision</u>	
		Actualiser			
		Revoir la configuration			
		Installer les licences			

On demande Ajouter au groupe

	Configuration SRV-DC1	×
Nom du serveur de Étendue de la déco Emplacement de la	licences : SRV-DC1 uverte : Domaine base de données : C:\Windows\System32\LServer\	Modifier l'étendue
Ce serveur groupe Ser Active Dire d'accès die présents d signaler l'ur par utilisate (SCP) dans figurera da de serveur	de licences ou le compte de service réseau n'est pas membre du veurs de licences Terminal Server dans les services de domaine ctory. Ce serveur de licences ne pourra pas accorder des licences nt aux services Bureau à distance par utilisateur aux utilisateurs ans le domaine, et vous ne serez pas en mesure de suivre ou de tilisation des licences d'accès client aux services Bureau à distance eur sur ce serveur de licences. de licences est inscrit en tant que point de connexion de service les services de domaine Active Directory. Le serveur de licences ns la liste des serveurs de licences connus de l'outil de configuration hôte de session Bureau à distance.	Ajo <u>u</u> ter au groupe
Et c'est tout !		
	Ce serveur de licences et le compte de service réseau sont membres Serveurs de licences Terminal Server dans les services de domaine A Directory. Ce serveur de licences pourra accorder des licences d'acco	du groupe ctive ès dient



Notre serveur est désormais opérationnel

ፍ				Gestionnaire de lice	ences
Action Affichage ?					
	Nom	État de l'activation	Étendue de la déco	Configuration	
	SRV-DC1	Activé	Domaine	ОК	



Id de serveur unique:

N.B: notre serveur de licence étant "unique", les licences installées ne seront valables que sur ce serveur...

L'ID de serveur unique	est d'ailleurs	visualisable dans	les propriétés du serveur
------------------------	----------------	-------------------	---------------------------

9				Gestionnaire de licences
Action Affichage ?				
🖅 🛱 Tous les serveurs	Nom	État de l'activation	Étendue de la déco	Configuration
	SRV-DC1	Activé	Domaine	OK
		Actualiser		
		Revoir la configuration		
		Installer les licences		
		Activer le serveur		
		Avancé	•	
		Créer un rapport	•	
		Supprimer des rapports .		
		Gérer les licences		
		Propriétés	•	

Dans l'onglet Méthode de connexion, on trouve ID du serveur de licences

Propriétés de : SRV-DC1				
Méthode de connexion Information	ons requises Informations facultatives			
Méthode de connexion :	Connexion auto. (recommandé) 🗸 🗸 🗸			
Description :	Ceci est la méthode recommandée. Le serveur de licences échangera automatiquement par Internet les informations requises avec le serveur Microsoft Clearinghouse.			
Configuration requise :	L'ordinateur doit pouvoir se connecter à Internet en utilisant une connexion SSL (Secure Sockets Layer).			
Choisir votre pays/région :	~			
ID de produit (Product ID) :	00252-70000-81458-AT518			
ID du serveur de licences :	DV49W-DWCWC-3XB6Q-4CFJ6-BHFHH-D2TPX-24M2			
	OK Annuler			



Migrer des licences :

Il faut sur le serveur activé demander clic droit gérer les licences

9.				Gestionnaire de licence
Action Affichage ?				
🗉 🛱 Tous les serveurs	Nom	État de l'activation	Étendue de la déco	Configuration
	SRV-DC1	Activé	Domaine	ОК
		Actualiser		
		Revoir la configuration		
		Installer les licences		
		Activer le serveur		
		Avancé	•	
		Créer un rapport	•	
		Supprimer des rapports	5	
		Gérer les licences	•	

On déclanche un assistant

	Assistant Gestion des licences	x
	Assistant Gestion des licences	
G	Cet Assistant vous aide à effectuer l'une ou l'autre des opérations suivantes : • Migrer les licences à partir d'un autre serveur de licences vers celui-ci	

On indique que l'on souhaite Migrer / remplacer l'ancien gestionnaire

Assistant Gestion des licences	×
Choix de l'action Choisissez la migration des licences ou la reconstruction de la base de données du serveur de licences.	
Migrer les licences à partir d'un autre serveur de licences vers celui-ci	
L'autre serveur de licences sera considéré comme le serveur de licences source dans cet Assistant.	
Selectionnez un motir de migration des licences :	

Que l'on repère soit par son nom / @ Ip s'il est encore en fonction, soit par son

identifi	ant	unique	ID du serveur de	licences :	JYBMW-94	HB2-HRTX7	-2QW4Y-PRKCJ	-229MX-4Q3XE
			Assis	tant Gestion	des licences		X	
		Informations s Foumit les in	ur le serveur de lice formations requises sur le	n ces source e serveur de licer	nces source.		9 ₁	
	•	Nom ou adresse srv-dc.cabare-ir	IP du serveur de licence ntra.net	es source :				
	•	Le serveur de Sélectionnez le Entrez l'ID du	e licences source spécifi e système d'exploitation o serveur de licences sour	é n'est pas dispo qu'utilise le serve ce :	nible sur le réseau ur de licences sou V	irce :		



Ensuite que cela se corse, pour la saisie des licences... (vu les différents types)

	Assistant Gestion des licences					×	
Programme Sélection	de licence nez le programn	ne de licence a	pproprié.			9	
Chaque c ordinateur posséder acheté vo	Chaque client qui se connecte à un serveur hôte de session Bureau à distance, ou à un ordinateur virtuel dans une infrastructure VDI (Microsoft Virtual Desktop Infrastructure) doit posséder une licence valide. Sélectionnez le programme de licence avec lequel vous avez acheté vos licences.						
Programm	e de licence :	Licence Ope	en) v			
Descriptio	n:	Inclut les offr de licence m	es Open Business e ultiple pour les petite	t Open Volume, progr es et moyennes entrep	ammes orises.		
Format et	emplacement :	Les numéros trouvent sur l numéro d'aut alphanumério chiffres) et le chiffres.	d'autorisation et de 'en tête de votre co orisation comprend jues (8 chiffres suivi numéro de contrat d	contrat de licence se nfirmation de commar quinze caractères s de 3 lettres suivies o de licence contient 8	nde. Le de 4		
Exemple :		12345678A	3C1234	(Numéro d'autorisa	tion)		
		12345678		(Numéro de licence	e)		
			Assistant	Gestion des li	rences	-	x
	_		Assistant	Cestion des in	tences		-
	Entrer le r	de licence numéro de con	trat.				۹ <mark>ـــ</mark>
	Entrez le numéro de contr votre programme de licence Programme de licence : Numéro de contrat :			ous avez acheté vos écédent. en IZE1510	s licences. Pour (Numéro d'aut (Numéro de li	modifier torisation) cence)	
			Assistant	Gestion des lie	cences		x
	Version du p Sélection	p roduit et ty nez la version	p e de licence du produit et le typ	e de licence.			9
	Sélectionnez la version du p		du produit et le typ	e de licence à instal	ler sur le serveur	de licences.	
	Programm	e de licence :	Licence Open				
	Version du	u produit :	Windows Server	2012		~	
	Type de licence :		Licence d'accès	utilisateur des servi	ces Bureau à dis	stance par 👻	
			Ce type de liceno est attribué à cha de session Burea Server 2012 R2, services Bureau Server 2012 R2.	ce d'accès client de aque utilisateur se cr au à distance Windo ou à un serveur hôt à distance Windows	s services Burea onnectant à un s ws Server 2012 e de virtualisatio s Server 2012 ou	au à distance serveur hôte ou Windows in des u Windows	
	Quantité :		5 (Nombre de licen de licences)	ices qui seront dispo	nibles à partir de	e ce serveur	

Et voilà nos 5 CAL transférées

%	Gestionnair	e de licences d	es services Bure	eau à distance		
Action Affichage ?						
E Tous les serveurs	Version et type de la licence	Programme de	Nombre total	Disponible	Émise	Date d'expirati
SRV-DC1	🖶 Windows 2000 Server - Licence d'accès u	Intégré	Illimité	Illimité	0	Jamais
Windows 2000 Server	🔄 Windows Server 2012 - Licence d'accès u	Ouvrir	5	5	0	Jamais
Windows Server 2012						



RDS 2012 R2 – accès intranethttp://www.cabare.netPage 48- SYS 32 – Cours TP - ver 1.3 -- Michel Cabaré -

Installer des licences :

Evidemment il faut les identifiants des CAL ou selon les type les identifiants de contrat...

Nindows Servers	Windows Server 2 Rights	012 RDS CALs Internal Use	Octrois de licences Action Pack
Vous bénéficiez des avanta participation au MPN : Microsoft Action Pack	ges liés aux droits d'utilisatic	n interne suivants grâce à votre	10 Licences
Produit	Sièges	Jeton	
Windows Server 2012 RDS CA	Ls 10	MKHNK-BH4Q3-J2P73-Q4BQT-QYFC4	Total : 10

Il faut sur le serveur activé demander clic droit **Installer les licences**

9				Gestionnaire de licences
Action Affichage ?				
🗉 🙀 Tous les serveurs	Nom	État de l'activation	Étendue de la déco	Configuration
	SRV-DC1	Activé	Domaine	OK
		Actualiser		
		Revoir la configuration .		
		Installer les licences Activer le serveur Avancé	•	
		Créer un rapport Supprimer des rapports	•	
		Gérer les licences		
		Propriétés		

Cela déclanche un assistant

Assistant Installation de licences	x
Assistant Installation de licences	
Cet Assistant installera des licences sur votre serveur de licences des services Bureau à distance.	

Ou il faut choisir le type de licence, par exemple un pack

	Assistant Installation de licences	x
Programme de licence Sélectionnez le programm	ne de licence approprié.	9
Chaque client qui se conr ordinateur virtuel dans un posséder une licence vali acheté vos licences.	necte à un serveur hôte de session Bureau à distance, ou à un e infrastructure VDI (Microsoft Virtual Desktop Infrastructure) doit ide. Sélectionnez le programme de licence avec lequel vous avez	
Programme de licence :	Pack de licence (vers. comm.)	
Description :	Cette licence a été achetée en quantité prédéfinie dans un magasin ou chez un distributeur. Le package peut s'appeler « Pack de licence client Microsoft Windows ».	
Format et emplacement :	Le code de licence contenu dans le Pack de licence sera demandé. Le code de licence est une suite de cinq jeux de cinq caractères alphanumériques.	



Assistant Installation de licences						
Code de licence Entrez le code de licence se trouvant dans le coffret de votre produit.						
Entrez le code de licence pour chaque licence que vous avez achetée, puis cliquez sur Ajouter après avoir entré chaque code de licence. Le code de licence contient 5 groupes de 5 caractères alphanumériques.						
Codes de licence entrés	:					
Code de licence MKHNKBH4Q3J2P73Q	4BQTQYFC4	État En attente	Type de produit Windows Server 2012			
	Assistant Inst	tallation de li	icences	x		
	Fin de l'Assistant Installation de licences					
	Vous avez terminé l'Assistant Installation de licences.					
Licences installées :						
U Windows Server 2012 - Licence d acces utilisateur des services Bureau à distance par utilisateur installés						
	< III >					

Et voilà nos 10 CAL installées

%	Gestionnaire de licences des services Bureau à distance					
Action Affichage ?						
🖃 🛱 Tous les serveurs	Version et type de la licence	Programme de	Nombre total	Disponible	Émise	Date d'expirati
SRV-DC1	🖶 Windows 2000 Server - Licence d'accès u	Intégré	Illimité	Illimité	0	Jamais
🦳 🖏 Windows 2000 Server	🖶 Windows Server 2012 - Licence d'accès u	Achat au détail	10	10	0	Jamais
	🖶 Windows Server 2012 - Licence d'accès u	Ouvrir	5	5	0	Jamais

N.B: on peut associer des licences utilisateurs à des comptes de l'AD spécifiques, "différents" des comptes de domaines utilisés pour les ouvertures de sessions.. par exemple 50 utilisateurs AD, et 10 utilisateurs CAL RDS autres... cela obligera à s'authentifier sur le portail WEB RDS ou le bureau a distance avec des comptes spécifiques, mais bon...



Informer le serveur RDSH de quel type de licence il a besoin

Il faut donc maintenant, pour notre **serveur Hôte RDSH**, c'est à dire le serveur hébergeant les services **RDS**, indiquer quel type de licence il doit demander

Sur le serveur hôte (et non pas sur le serveur de licence) dans le Gestionnaire de serveur, Services Bureau à distance, Vue d'ensemble on va dans taches et on demande Modifier les propriétés de déploiement



Et on se place sur gestionnaire de licence

b	Propriétés de déploiement	x
Configurer le dép Afficher tout Passerelle des serv + Gestionnaire de lic – Accès Web des ser + Certificats +	Propriétés de déploiement Ioiement Gestionnaire de licences des services Bureau à distance Sélectionnez le mode de licence des services Bureau à distance : O Par périphérique Par utilisateur Spécifiez un serveur de licences puis cliquez sur Ajouter : Ajouter	X
	Choisissez l'ordre des serveurs de licences des services Bureau à distance : Le serveur hôte de session Bureau à distance ou le serveur hôte de virtualisation des services Bureau à distance envoie les demandes de licences aux serveurs de licences spécifiés dans l'ordre où ils sont répertoriés.	

et Il faut ici indiquer si on veut des licences RDS du genre **Par périphérique** (non poste) ou **par utilisateur** (login de domaine)

P		Propriétés de déploiement	_ D X
Config Passere Gestion Accès V Certific	urer le déplo Afficher tout Ille des serv + Inaire de lic – Veb des ser + ats +	Propriétés de déploiement Diement Gestionnaire de licences des services Bureau à Sélectionnez le mode de licence des services Bureau à distance : O Par périphérique Par utilisateur Spécifiez un serveur de licences puis cliquez sur Ajouter : Choisissez l'ordre des serveurs de licences des services Bureau à dis Le serveur hôte de session Bureau à distance ou le serveur hôte de services Bureau à distance envoie les demandes de licences aux ser spécifiés dans l'ordre où ils sont répertoriés.	Ajouter Ajouter etance : virtualisation des veurs de licences
		srv-dc I.cabare-intra.net	Monter



N.B: au niveau des Types de licence on ne peut pas mélanger les deux types sur notre serveur RDS ! (même si le serveur de licence / CAL lui peut le faire)

Sélectionnez le mode de licence des services Bureau à distance :

- Les CALS sont vendues par O Par périphérique ◄--paquets de 5
- Par utilisateur

Et voila au final à quoi cela peut ressembler.

A		Propriétés de déploiement
C	Configurer le dépl	oiement
•	Afficher tout Passerelle des serv + Gestionnaire de lic – Accès Web des ser + Certificats +	Gestionnaire de licences des services Bureau à distance Sélectionnez le mode de licence des services Bureau à distance : O Par périphérique O Par utilisateur Spécifiez un serveur de licences puis cliquez sur Ajouter : Ajouter
		Choisissez l'ordre des serveurs de licences des services Bureau à distance : Le serveur hôte de session Bureau à distance ou le serveur hôte de virtualisation des services Bureau à distance envoie les demandes de licences aux serveurs de licences spécifiés dans l'ordre où ils sont répertoriés.
		srv-dc1.cabare-intra.net Monter Descendre Supprimer

Dans l'exemple on a choisit ici

- de travailler avec des CAL utilisateur
- notre serveur de licence se trouve sur notre serveur DC. •



INSTALLER DES APPLICATIONS SUR LE RDS

Installation d'applications Mode Execute - install

On a vérifié qu'un utilisateur pouvait se connecter sur notre serveur RDS à travers le bureau à distance, cependant pour l'instant sur le bureau il n'y a pas d'application...

Normal, on n'a pas installé d'applications sur notre serveur...

La règle étant que les applications doivent être installées sur un Serveur, uniquement lorsque le rôle **RDS Bureau à Distance** est <u>déjà installé</u>...

N.B: pour office on ne peut installer que des versions Licence Volume...

Le Serveur RDS à 2 modes de fonctionnement et un mode maintenance

- Le mode **Execute** : dans lequel il peut lancer les applications pour ses clients
- Le mode Intall : utilisé pour effectuer les installations des applications

Et un mode dit « maintenance » dans lequel il refuse les connexions

Commande Change user

La commande change user permet de gérer la bascule entre les 2 modes de fonctionnement de notre serveur RDS.



Normalement par défaut un Serveur RDS est en mode **Execute**. Cela peut se vérifier en ligne de commande par

change user /query

comme dans

C:\Users\Administrateur.CABARE-INTRA>change user /query Le mode Exécution d'application est activé.

avant d'installer une application, il faut passer le serveur en mode **install** par la commande

change user /install

comme dans

3:\Users\Administrateur.CABARE-INTRA≻change user ∕install Session utilisateur prête à installer des applications.

on installe l'application voulue normallement par exemple ici office 2010

setup.exe

🛛 🛃 Lecteur de DVD (D:) OFFICE14



puis, après redémarrage éventuel on repasse si besoin le serveur en **mode execute** par la commande (Même si parfois le redémarrage peut refaire basculer le serveur en mode execute automatiquement...)

change user /execute

C:\Users\Administrateur.CABARE-INTRA>change user ⁄execute Session utilisateur prête à exécuter des applications.

Assistant Ajout programmes

Si on ne veut pas utiliser la ligne de commande change user... on peut utiliser un assistant graphique.

Dans le panneau de configuration en mode petites icones on trouve on trouve Installer une application sur un serveur Bureau à distance

Dans le panneau de configuration, à condition de ne pas être en mode détaillé, dans Programmes



on trouve Installer une application sur

un serveur Bureau à distance



Il faut aller chercher le setup du programme d'installation

N.B : à la fin de l'installation il faut bien fermer l'assistant...





Mode maintenance

via la commande graphique Dans le **gestionnaire de Serveur**, on se place sur la **collection**,



Sur le Serveur hôte et via clic droit on demande Ne pas autoriser les nouvelles connexions

SERVEURS HÔT Dernière actualisat	TES ion le 22/05/2016 12:53:13 Tous les	serve TÂCHES	•
Filtrer		. ⊕ .	۲
Nom du serveur	Туре	Bureaux virtuels	Auto
RDS-FORM	Hôte de session Bureau à distance	N/A	Vrai
	Ne pas autoriser les nouvelles co	onnexions	

On confirme la viande dur serveur RDSH

Ne pas autoriser les nouvelles connexions
Aucune nouvelle connexion ne peut être créée sur le serveur RDS-FORM.FORM.EDU. Voulez-vous vraiment continuer ?
Qui <u>N</u> on

Pour ré accepter les connexions, on repasse par clic droit Autoriser les nouvelles collections ATTENTION BUG d'affichage !



Et on retrouve alors

SERVEURS HÔTES Dernière actualisation le 22/05/2016	12:58:04 Tous les	se TÂCHES 🔻
Filtrer		
Туре	Bureaux virtuels	Autoriser les nouvell
Hôte de session Bureau à distance	N/A	Vrai



On peut aussi travailler en invite de commande par **chglogon** comme dans **chglogon /query**... pour savoir dans quel état on est

C:\Users\Administrateur.CABARE-INTRA>chglogon /query Les ouvertures de session sont actuellement ACTIVÉES

si on veut passer en mode maintenance on demande simplement

chglogon /drain voire chglogon /drainuntilrestart

comme dans

C:\Users\Administrateur.CABARE-INTRA>chglogon /drain Les nouvelles ouvertures de session d'utilisateur sont DÉSACTIVÉES, mais les rec onnexions aux sessions existantes sont ACTIVÉES.

puis pour ré-autoriser les connexions

chglogon /enable

comme dans

C:\Users\Administrateur.CABARE-INTRA>chglogon ⁄enable Les ouvertures de session sont actuellement ACTIVÉES

Installer – publier – Distribuer

Le fait d'avoir installé les programmes sur le serveur DRSH ne rend pas le bureau à distance plus ... « riche »

Encore faut il publier les ressources et décider ensuite de les distribuer d'une manière ou d'un autre pour en permettre l'utilisation conviviale

Cf chapitre suivant Applications et RemoteApp

Programmes et Certificats

Si on envisage d'installer des **Certificats** pour le fonctionnement plus convivial des **Remote Apps**, il serait bon de la faire **AVANT** d'installer les applications.

Par conséquent ne pas installer un panel d'application PUIS les certificats... on en installe éventuellement 1 pour tester le serveur RDS mais pas plus.



PROFILS UTILISATEURS

Les profils sur un serveur RDS :

Les profils RDS des utilisateurs sont stockés par défaut sur le serveur RDS de manière tout à fait analogue aux profils utilisateurs crées lors des ouvertures de session sur n'importe quelle machine... Donc

- si on s'authentifie localement sur un poste p1, le profil est stocké physiquement sur le poste p1 (et corresponds au compte local)
- si on s'authentifie sur un domaine depuis un poste p1, le profil est stocke physiquement sur le poste p1 (et corresponds au compte de domaine)
- si on s'authentifie via une connexion RDP, le profil de l'utilisateur de domaine est stocké localement sur le serveur RDP qui a répondu.

Ce qui fait que sur le serveur RDS, les utilisateurs qui ont ouvert une session via RDP ont un profil "exactement" comme ceux qui ont ouvert une session locale



Ce qui n'est pas très judicieux... si on change de serveur RDS, ou si on en ajoute un deuxième, ou l'on veut accéder à ses documents ensuite, cela peut poser problème...

Objectif des profils itinérants :

Si on a un seul serveur RDS...ll n'y a pas forcément besoin de gérer les profils RDS utilisateurs, qui sont stockés par défaut sur le serveur RDS

Le seul cas ou cela devient impératif, c'est lorsque l'on a deux serveurs RDS minimum, avec du **Load balancing**.

En effet dans ce cas, au cours d'une journée l'utilisateur peut très bien ouvrir des sessions alternativement sur un serveur, puis un autre...

Il est important dans ce cas de créer des profils itinérants pour les profils utilisateurs entre les deux serveurs RDS...

N.B : la création de profils itinérants ne supprime pas la création du profil loca! simplement celui-ci est recopié aussi sur un espace réseau !



Les profils itinérants standards (rappel) :

La construction d'un profil itinérant va reposer sur 2 actions:

- La création et le partage d'un dossier de stockage
- Renseignement pour chaque compte utilisateur de l'existence de cet emplacement

Création du dossier partagé stock-profil

Au niveau du partage, préférer un groupe **utilisateur** au groupe par défaut prédéfini **tout le monde**

3. Autorisations pour stock-profils	Autorisations pour stock-profils
Autorisations du partage Noms de groupes ou d'utilisateurs : Image: Supprime transmission of the second se	Autorisations du partage Noms de groupes ou d'utilisateurs : Utilisateurs (CABARE-INTRA\Utilisateurs) Ajouter
Autorisations pour Tout le monde Autoriser Refuser	Autorisations pour Utilisateurs Autoriser Refuser
Contrôle total	Contrôle total
Modifier 🗌 🗌	Modifier 🗹 🗌
Lecture 🗹 🗌	Lecture 🗹 🗌

Renseignement du compte utilisateur comme quoi il doit utiliser un profil itinérant . Effectuer un clic droit sur l'utilisateur **Propriétés** / onglet **Profil** et au niveau du champ **Chemin du profil** on indique

\\nom-srv\nom-partage\%username%

	Propriétés de : stg1						x			
Γ	Environnement Sessions Contrôle à distance Profil des services Bureau à distance COM+						COM+			
	Profil utilisateur									
Chemin du profil : \\nom-srv\nom-partage\% Script d'ouverture de			e\%usemame`	%						
	Dossier de base									
	٥	hemin d'a	accès local	:						
	00	onnecter	:	¥ à:						

On indique simplement le chemin UNC vers le serveur, suivi du partage et de la variable **%username%** qui prendra pour valeur le login de l'utilisateur

- l'utilisateur utilise un PC s XP, le dossier créé sera nommée login
- l'utilisateur utilise un PC Seven (mini) le dossier sera nommé login.v2

N.B : Il existe une incompatibilité entre vista/7 et 2008/2008r2

N.B : A ce titre la **redirection de dossier**, (pour le dossier mes documents par exemple), peut permettre à des utilisateurs travaillant sur des versions clientes différentes de retrouver leurs fichiers ! et **allège la taille des profils**



Les profils itinérants RDS par GPO

le dossier partagé pour héberger les profils utilisateurs RDS étant crée...

par exemple stock-profil-rds sur un					
serveur de fichier, on pose des					
autorisations de partage pour le					
groupe utilisateurs du domaine					
(plutôt que pour Tout le monde)					

N.B : s'assurer que l'on n'ait pas de synchronisation de fichier, ou de versions précédentes activées

👃 🛛 Autorisations pour	stock-profil-	rds X
Autorisations du partage		
Noms de groupes ou d'utilisateurs :		
& Utilisateurs du domaine (FORM\	Utilisateurs du dor	maine)
	Ajouter	Supprimer
Autorisations pour Utilisateurs du domaine	Autoriser	Refuser
Contrôle total	✓	
Modifier	\checkmark	
Lecture	✓	

On travaille ensuite par **GPO ordinateur**, et non plus par modification du **compte utilisateur**, onglet **profil**, et cette **GPO** il faudra l'appliquer à tous serveur **RDS** recevant la demande de connexion

Donc il faut créer 1 **GPO ordinateur**, s'appliquant au serveur RDS redirigeant le profil utilisateur RDS... △ Objets de stratégie de groupe
 Default Domain Controllers Policy
 ☑ Default Domain Policy
 ☑ strat-ordi-profils-rds
 ☑ strat-ord-mot-de-passe-simple
 ☑ strat-util-office-2010

Par exemple strat-ordi-profils-rds

Il faut ensuite appliquer cette GPO <u>sur notre</u> <u>serveur RDS</u>.

N.B: à terme si on dispose de plusieurs serveurs RDS, il est bon de les stocker dans la même UO pour qu'ils récupèrent plus facilement les mêmes GPO.

Utilisateurs et ord	dinateurs Active Directory
Fichier Action Affichage ?	
🗢 🔶 📶 🤞 📋 🗙 🗐 Q 📑 🛛 🖬 🖏	k 🛅 🔻 🔟 🖗
Serveur-new-ped	Nom Type
srv-physiques	🖳 srv-rds1 Ordinateur
⊿ 📓 srv-vm	
vm-pour-acces-rds	

Donc si on a cette **UO** nommée **vm-pour-acces-rds** dans l'**AD** alors il faut appliquer une **GPO** par exemple **strat-ordi-profil-rds**

⊿ Srv-vm
 ⊿ S vm-pour-acces-rds
 , strat-ordi-profils-rds



Réglage GPO

Note GPO doit contenir au minimum

dans les Modèles d'administration / Composants Windows / Services Bureau à Distance on trouve alors dans Hôte de la session bureau à distance / Profils

🔺 🦳 Services Bureau à distance	^	Paramètre	État
Client Connexion Bureau à distance		E Limiter la taille de l'ensemble du cache des profils utilisateur	Activé
🧮 Gestionnaire de licences des services Bu		E Définir le répertoire de base de l'utilisateur des services Bure	Non configuré
🔺 🚞 Hôte de la session Bureau à distance		Utiliser les profils obligatoires sur le serveur Hôte de la sessio	Non configuré
Compatibilité des applications		Définir le chemin d'accès au profil utilisateur itinérant des se	Activé
Connexions			
🧮 Délais d'expiration des sessions			
Dossiers temporaires			
Environnement de session à distanc			
🧮 Gestionnaire de licences			
Profils			

On modifie **Définir le chemin d'accès au profil utilisateur itinérant des services Bureau à distance.**

Paramètre précéd	ent Paramètre sui	ıt
O <u>N</u> on configuré	Commentaire :	
• <u>A</u> ctivé		
O <u>D</u> ésactivé		
	Pris en charge sur :	Au minimum Windows Server 2003
Options :		Aide :

On modifie Limiter la taille de l'ensemble du cache des profils utilisateurs...

9	Limiter la taille de	l'ensemble du cache des profils utilisateur itinérant 🛛 💻 🗖	x
📑 Limiter la taille (de l'ensemble du cache	des profils utilisateur itinérant Paramètre précédent Paramètre suivan	t
 Non configuré Activé 	Commentaire :		^
 Désactivé 	Pris en charge sur :	Au moins Windows Server 2008 R2	~ ~
Options :		Aide :	
Intervalle d'analyse 15 Taille maximale du o 5	(minutes) : cache (Go) :	\Modèles d'administration\Système\Profils utilisateur. Si vous activez ce paramètre de stratégie, vous devez spécifier un intervalle d'analyse (en minutes) et une taille maximale (en giga-octets) pour l'ensemble du cache du profil utilisateur itinérant. L'intervalle d'analyse détermine la fréquence à laquelle la taille de l'ensemble du cache du profil utilisateur itinérant est vérifiée. Lorsque la taille de l'ensemble du cache du profil utilisateur itinérant dépasse le seuil maximum prévu, les profils utilisateur itinérant plus anciens (c'est-à-dire ceux utilisés le moins récemment) sont supprimés jusqu'à ce que la taille du cache soit inférieure à la limite maximale spécifiée.	^



dans les Modèles d'administration / Composants Windows / système on trouve dans Profils utilisateurs / Planifier le téléchargement en tache de fond

Planifier le téléchargement en tâ	e de fond du fichier de Registre d'un profil util	is 😑 🗖 🗙
Planifier le téléchargement en tâche de fono Paramètre précédent	u fichier de Registre d'un profil utilisateur itinérant au cou	urs d'une session
 Non configuré Commentaire : Activé Désactivé 		^
Pris en charge sur :	minimum Windows Server 2008 R2 ou Windows 7	×
Mode de planification : Exécuter à intervalle régulier v Seuls les paramètres suivants sont exigés et applicables En cas de sélection de l'option « Exécuter à intervalle régulier ». Intervalle (heures) : 1 vices et Seuls les paramètres suivants cont evicés et	 Ce paramètre de stratégie planifie le télécharge fond du fichier de Registre d'un profil utilisateu (ntuser.dat). Ce paramètre de stratégie contrôle téléchargement du fichier de Registre d'un pro itinérant (les autres données utilisateur et les pr sont pas téléchargés) et ne le télécharge que si ouvert une session. Ce paramètre de stratégie r téléchargement du fichier en question si l'utilis déconnecte avant la fin de l'opération. Si vous sélectionnez l'option « Exécuter à interv vous devez spécifier une valeur comprise entre 	ment en tâche de Ir itinérant e uniquement le fil utilisateur rofils standard ne 1'utilisateur a n'interrompt pas le sateur se /alle régulier », 1 et 720 heures.

dans les Modèles d'administration / Composants Windows / système on trouve dans Stratégies de groupe / Autoriser un traitement asynchrone de la stratégie de groupe utilisateur lors d'une ouverture de session par le biais des services bureau à distance

& Autoriser un traitement asynchro	one de la stratégie de groupe utilisateur lors d'une o	x
Autoriser un traitement asynchrone de la s services Bureau à distance	tratégie de groupe utilisateur lors d'une ouverture de session par le biais des	
Paramètre précédent Paramètre suiv	/ant	
O Non configuré Commentaire :		^
 Activé 		
O Désactivé		~
Pris en charge sur :	Au minimum Windows Server 2008	
		~
Options :	Aide :	
	Ce paramètre de stratégie permet à Microsoft Windows de traiter les paramètres de stratégie de groupe utilisateur de façon asynchrone lors d'une ouverture de session par le biais des services Bureau à distance. Le traitement asynchrone de la	^



RDS 2012 R2 – accès intranet - SYS 32 – Cours TP - ver 1.3 - Si on souhaite en tant d'administrateur accéder au contenu des dossiers des profils itinérant, il est nécessaire de configurer une GPO qui devra s'appliquer à tous les ordinateurs (clients et serveur):

Configuration ordinateurs/Stratégies/Modèles d'administration/Système/Profil des utilisateurs/Ajouter le groupe de sécurité administrateur aux profils itinérants utilisateurs

Se Ajouter le groupe de sécur	ité Administrateurs aux profils utilisateur itinérants 🛛 💻 🗙
Ajouter le groupe de sécurité Admini Paramètre précédent Paramètre su	strateurs aux profils utilisateur itinérants ivant
O Non configuré Commentaire :	
 Activé 	
○ Désactivé	
Pris en charge sur :	Au minimum Windows Server 2003 ou Windows XP Professionnel
	×
Options :	Aide :
	Si vous activez ce paramètre de stratégie, le groupe ^ Administrateurs reçoit également le contrôle total sur le dossier ^ de profil de l'utilisateur.

Désormais si Bob ouvre une session RDS cela génère dans notre dossier la structure suivante, typique des profils errants.

⊿ 🍌 stoc	k-profil-rds		bob.FORM	A.V2	L	Propriétés de : bo	b.FORM.V2	X
Et si admir itinéra Et bien qualité personr	on l'o histrateurs nt sûr selor de la co haliser soi	a de s on a n les r onnex n profi	églages e ion bob p	les rofil t la eut	Général Partage Sé Nom de l'objet : C:vi Noms de groupes ou d Système bob (bob@form.e) Administrateurs (F Pour modifier les autori Autorisations pour Adm Contrôle total Modification	curité Versions précédente tock-profil-rds'bob.FORM.V. utilisateurs : Ju) DRMVAdministrateurs) nations, cliquez sur Modifier. inistrateurs	es Personnaliser 2 Autoriser V	Modifier r Refuser
	Affichage Re Performance:	Conne> A dist essources lo s idiquez votrr eformances Haut débit (2 utoriser les f	tion Bureau à tion Bureau tance cales Programmes e vitesse de connexio 2 Mbits/s - 10 Mbits/s onctionnalités suivan n du Bureau	a distance	Avancé <>			



Animation des menus et des fenêtres

Afficher le contenu des fenêtres pendant leur

Lissage des polices
 ✓ Composition du Bureau

déplacement

Styles visuels

Profil itinérants problèmes réglages supplémentaires

N.B: quelques réglages supplémentaires bénéfiques en cas de problèmes avec les profils temporaires

Service de profil utilisateur 👋 🗴
Un problème relatif à votre profil itinérant a été rencontré. La connexion a été établie avec votre profil
local précédemment enregistré. Consultez le journal des événements pour obtenir des détails ou contactez votre administrateur.
6

Profi	l des utilis	ateurs		×
Un profil utilisateur si d'autres informations pouvez créer un prof utilisez ou vous pouv même partout.	tocke les para i liées à votre îl différent sur ez sélectionne	mètres de compte d r chaque (er un prof	e votre Bure íutilisateur, ordinateur q il itinérant q	au et Vous µe vous µi sera le
Profils enregistrés sur cet ordi	nateur :			
Nom	Taille	Туре	Statut	Mo
CABARE-INTRA \Administ	?	Local	Local	14
IIS APPPOOL \.NET v4.5	58,9 Mo	Local	Local	13

Dans Système/Ouverture de session 1 réglage

Ouverture de session		
Sélectionnez un élément pour obtenir	Paramètre 🔹	État
une description.	E Toujours utiliser un arrière-plan d'ouverture de session pers	Non configuré
	Toujours utiliser l'ouverture de session classique	Non configuré
	Toujours attendre le réseau lors du démarrage de l'ordinate	Activé
	🗈 Ne pas traiter la liste d'exécution unique	Non configuré

System/Logon "Always wait the network at computer start up and logon" -> Enabled

Toujours attendre le réseau lors	du démarrage de l'ordinateur et de l'ouverture de s 😑 🗖 🗙
Toujours attendre le réseau lors du dé Paramètre précédent Paramètre suiv	marrage de l'ordinateur et de l'ouverture de session
 Non configuré Commentaire : Activé Désactivé Pris en charge sur : 	Au minimum Windows Server 2003 ou Windows XP Professionnel
Options :	Aide :
	Si le serveur est configuré comme suit, ce paramètre de stratégie est pris en compte au moment du traitement de la stratégie de groupe lors de l'ouverture de session de l'utilisateur : • Le serveur est configuré en tant que serveur Terminal Server (autrement dit, le service de rôle Terminal Server est installé et configuré sur le serveur) ; et • Le paramètre de stratégie « Autoriser un traitement asynchrone de la stratégie de groupe utilisateur lors d'une ouverture de session par le biais des services Terminal Server » est activé. Ce paramètre de stratégie se trouve sous Configuration ordinateur \Polices\Modèles d'administration\Système\Stratégie de groupe\. Si cette configuration n'est pas implémentée sur le serveur, le paramètre de stratégie est ignoré. Dans ce cas, le traitement de la stratégie de groupe lors de l'ouverture de session utilisateur est synchrone (ces serveurs attendent que le réseau soit initialisé lors de l'ouverture de session de l'utilisateur).
	OK Annuler Appliquer



Dans Windows Components/RDS/RDSH/Connections 3 réglages

Sélectionnez un élément pour obtenir une description.	Paramètre 📩	État
	🗄 Autoriser le démarrage distant de programmes non répertor	Non configuré
	🗄 Autoriser les utilisateurs à se connecter à distance à l'aide de	Non configuré
	E Configurer l'intervalle de conservation des connexions	Désactivé
	🗈 Définir les règles pour le contrôle à distance des sessions util	Non configuré
	🗈 Désactiver la planification de répartition de charge équilibré	Non configuré
	🗈 Limiter le nombre de connexions	Non configuré
	🗈 N'autoriser qu'une session de services Bureau à distance par	Activé
	🗈 Reconnexion automatique	Désactivé
	🖹 Refuser la déconnexion d'un administrateur connecté à la se	Non configuré
	Sélectionner des protocoles de transfert RDP	Non configuré
	Sélectionner la détection du réseau sur le serveur	Non configuré
	Suspendre la connexion de l'utilisateur pour terminer l'inscri	Non configuré

Windows Components/RDS/RDSH/Connections "Automatic reconnection" -> Disabled

	seconnexion automatique					
Reconnexion au	tomatique	Paramètre précédent Paramètre suivant				
 Non configuré Activé 	Commentaire :		^			
Oésactivé	Pris en charge sur :	Au minimum Windows Server 2003 ou Windows XP Professionnel	~ ~			
Options :		Aide :				
		Indique si les clients Connexion Bureau à distance doivent être autorisés à se reconnecter automatiquement aux sessions d'un serveur Hôte de la session Bureau à distance si leur liaison réseau est temporairement perdue. Par défaut, vingt tentatives de reconnexion au maximum sont effectuées à des intervalles de cinq secondes.	^			

Windows Components/RDS/RDSH/Connections "Configure keep-alive connection interval" -> Disabled

💭 Configurer l'intervalle de conservation des connexions 📃 🗕 🗖 🗙					
Configurer l'inte	rvalle de conservation	des connexions Paramètre précédent Paramètre suivant			
○ Non configuré	Commentaire :	<u>^</u>			
○ Activé					
Désactivé		×			
	Pris en charge sur :	Au minimum Windows Server 2003			
		×			
Options :		Aide :			
Intervalle de conservation de connexion active :		Après la perte de la connexion à un serveur Hôte de la session Bureau à distance par un client Hôte de la session Bureau à distance, la session sur le serveur Hôte de la session Bureau à distance peut rester active au lieu de passer à un état déconnecté, même si le client est physiquement déconnecté du serveur Hôte de la session Bureau à distance. Si le client se connecte à nouveau sur le même serveur Hôte de la session Bureau à distance, une nouvelle session est susceptible d'être établie (si le serveur Hôte de la session Bureau à distance est configuré pour autoriser plusieurs sessions), et la session d'origine peut être encore active.			



Windows Components/RDS/RDSH/Connections "Restrict RDS users to a single RDS Session" -> Enabled

N'autoriser qu'une session de services Bureau à distance par utilisateur 💶 🗖 🗙						
N'autoriser qu'une session de services Bureau à distance par utilisateur Paramètre précédent Paramètre suivant						
 Non configuré Commentaire : Activé Désactivé 						
Pris en charge sur :	Au minimum Windows Server 2003					
	Ce paramètre de stratégie vous permet de limiter les utilisateurs à une seule session de services Bureau à distance. Si vous activez ce paramètre de stratégie, les utilisateurs qui ouvrent une session à distance via les services Bureau à distance sont limités à une seule session (active ou déconnectée) sur ce serveur. Si l'utilisateur quitte la session dans un état déconnecté, il se reconnecte automatiquement à cette session lors de la prochaine ouverture de session.					

Dans Windows Components/RDS/RDSH/dossiers temporaires 1 réglage

Dossiers temporaires		
Ne pas supprimer les dossiers	Paramètre 🔶	État
temporaires en quittant	📄 Ne pas supprimer les dossiers temporaires en quittant	Désactivé
	🗈 Ne pas utiliser les dossiers temporaires par session	Non configuré
Modifier le paramètre de stratégie	^	

Windows Components/RDS/RDSH/Temporary Folders "Do not delete temp folders upon exit" -> Disabled:

se Ne pas supprimer les dossiers temporaires en quittant 📃 🗖 🗙					
📷 Ne pas supprim	er les dossiers tempora	es en quittant Paramètre préc	édent Paramètre suivant		
 Non configuré Activé Décactivé 	Commentaire :		<u>`</u>		
C Desactive	Pris en charge sur :	Au minimum Windows Server 2003	^ ~		
Options :		Aide :			
		Si vous activez ce paramètre par session d'un utilisateur s session. Si vous désactivez ce param temporaires sont supprimés session, même si l'administr autrement.	e de stratégie, les dossiers temporaires sont conservés lorsqu'il ferme sa ètre de stratégie, les dossiers ; lorsqu'un utilisateur ferme une rateur du serveur en décide		



UPD USER PROFILS DISKS

UPD ou disques profils utilisateurs:

Cette nouvelle solution apparaît avec le rôle RDS 2012 pour les deux scénarios de déploiement : Session & VDI.

Il s'agit de « **UPD** : **U**ser **P**rofils **D**isks », cette fonctionnalité permet de stocker d'une manière centralisée les données des utilisateurs et des applications dans un seul disque virtuel (VHDx) dédié à chaque profil utilisateur.

- Quand un utilisateur distant ouvre une Session sur un serveur RDSH ou lance un Programme RemoteApp, son disque de profil associé <u>est</u> <u>attaché</u> à sa session,
- Il est ensuite <u>détaché</u> lors de la fermeture de sa session

Avec ce processus, aucune donnée n'est copiée à l'ouverture et fermeture de la session, ce qui permet d'éviter les erreurs de récupération et synchronisation connues avec les Profils Itinérants.

Configuration minimale:

Basiquement, il faut un serveur RDS et un espace partagé :

- Un espace partagé
- Un gestionnaire de serveur depuis un serveur RDS ayant au minimum les 3 rôles RDSH – RDCB et RDWA

On va se créer dans l'exemple un dossier **stock-upd-rds** que l'on va partager pour les utilisateurs du domaine

CePC Disque local (C:) stock-upd-rds

Autorisations point	ur stock-upd-r	ds ×
Autorisations du partage		
Noms de groupes ou d'utilisateurs :		
& Utilisateurs du domaine (FORN	1\Utilisateurs du dor	maine)
	Ajouter	Supprimer
Autorisations pour Utilisateurs du domaine	Autoriser	Refuser
Contrôle total		
Modifier		
Lecture	~	

On va dans le Gestionnaire de Serveur

du serveur RDS et on se place sur la collection voulue Modifier les propriétés

• • Collections • QuickSessionCollection					
Vue d'ensemble	PROPRIÉTÉS Propriétés de la co	llection	TÂCHES 🔻	CONNI Dernière	
Serveurs	Type de collection	Session	Modifier le	es propriétés	
Collections	Ressources	Programmes RemoteApp		runer	
QuickSessionCollection	Groupe d'utilisateurs	FORM\Utilisateurs du domaine		Nom d	



RDS 2012 R2 – accès intranet - SYS 32 – Cours TP - ver 1.3 -

http://www.cabare.net Page 66 - Michel Cabaré -

Dans les propriétés de la collection il faut autoriser les User Profil Disks, en indiquant un emplacement et une taille maximale

	L	QuickSessionCollectio	on Propriétés	_ 0	x	
	Collection de sessions					
	Afficher tout Général + Di Groupes d'utilisate +	Afficher tout H Disques de profil utilisateur d'utilisate +				
	Session + Les Sécurité + et l Équilibrage de la c + doi l'ut Paramètres du clie + Disques de profil	disques de profil utilisateur : dossiers à un emplacement es disques de profil utilisate vent disposer du contrôle to ilisateur actuel doit être mer <u>A</u> ctiver les disques de profil Emplacement : \\dc-form\stock-upd-rd	permettent aux utilisateurs de stoa : central. Vous pouvez activer la rec ur dans une collection. Les serveur: tal sur le partage du disque de pro mbre du groupe Administrateurs lo utilisateur	cker des paramètres e direction de dossiers s de la collection ofil utilisateur, et ocal sur ce serveur.	t =	
		Taille maximale (en Go) :				
Si celo	a fonctionne cela	4	Propriétés de : stock-upd	l-rds	×	
modifi dossie pour t	e les droit d'accès NTFS (r partagé, en Contrôle To ous les serveurs RDS,	Général Partage Nom de l'objet : O tal Noms de groupes ou & CREATEUR P Système & RDS-FORMS Système & Utilisateurs (FO Pour modifier les aut Autorisations pour R Contrôle total	Sécurité Versions précédentes Person C:\stock-upd-rds u d'utilisateurs : ROPRIETAIRE (FORM\Administrateurs) RM\Utilisateurs) orisations, cliquez sur Modifier. DS-FORM\$	nnaliser Modifier. Autoriser Refuse		
Et les autorisations de partage également Mutorisations pour stock-upd-rds Autorisations du partage Noms de groupes ou d'utilisateurs : RDS-FORMS Utilisateurs du domaine (FORM\Utilisateurs du domain					×	
(si on ajoute des serveurs RDSH supplémentaires dans le déploiement, l'assistant configure automatiquement leurs droits d'accès (Partage & permissions NTFS) au niveau du partage spécifié sur les UPDs)				Ajouter Suppri Autoriser Refuse	mer r	

Et crée un fichier UVHD-template.vhdx dans le partage





Fichier UVHD-s1-xxxx:

Chaque utilisateur qui ouvrira une session se verra créer un fichier **.vhdx**, crée à partir de son **SID**

Dis	sque local (C:) → stock-upd-rds v C Rec
^	Nom
	👝 UVHD-S-1-5-21-1970175263-3814210957-2855509778-1108.vhdx 🚽
	👝 UVHD-S-1-5-21-1970175263-3814210957-2855509778-1111.vhdx
	iggi UVHD-template.vhdx

Il n'y a plus de profil utilisateur enregistré en tant que tel sur le Serveur RDS

Profil des utilisateurs

Un profil utilisateur stocke les paramètres de votre Bureau et d'autres informations liées à votre compte d'utilisateur. Vous

même partout.

pouvez créer un profil différent sur chaque ordinateur que vous utilisez ou vous pouvez sélectionner un profil itinérant qui sera le

X

Et physiquement l'ancien profil de bob est renommé **bob.BACKUP-0**

4 📜 Utilicatours				Profils enregistrés sur cet ordinateur :				
	NO	om		Nom	Taille	Туре	Statut	Mo
NET v4.5				FORM\Administrateur	9,63 Mo	Local	Local	23
 NET v4.5 NET v4.5 Classic Administrateur Administrateur.FORM All Users bob.BACKUP-0 		.NET v4.5 .NET v4.5 Classic Administrateur Administrateur.FOF All Users bob.BACKUP-0		FORM\Administrateur FORM\toto IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 NT SERVICE\MSSQL\$MIC Profil par défaut RDS-FORM\Administrateur	9,63 Mo 9,23 Mo 57,7 Mo 57,7 Mo 58,4 Mo 57,4 Mo 57,9 Mo	Local Itinér Local Local Local Local Local	Local Itinér Local Local Local Local	23 23 19 19 23 18 19
 Default Default User MSSQL\$MICROSOFT##WID Public Contemporation 	2	Default Default User MSSQL\$MICROSOF Public						

N.B : Copie des dossiers / déplacement

Il s'agit de fichier avec de la protection NFTS, par conséquent XCOPY est nécessaire si on restedans le même lecteur (déplacement)

xcopy c:\ancien c:\noucveau /O /X /E /H /K

/E – Copies folders and subfolders, including empty ones.

- /H Copies hidden and system files also.
- /K Copies attributes. Typically, Xcopy resets read-only attributes.
- **/O** Copies file ownership and ACL information.
- /X Copies file audit settings (implies /O).

Si l'utilisateur n'est pas connecté, il est tout a fait possible de **monter** le disque profil comme n'importe quel disque **.vhdx**

۰D	isque local (C:) → stock-upd-rds		~ C	Re
^	Nom	•		
GUVHD-S-1-5-21-1970175263-3814210957-2855509778-11				
	👝 UVHD-template.vhdx	Monter		
			Ouvrir avec	

N.B : ne pas oublier de l'éjecter ensuite



Options UPD:

On souhaite minimiser le profil stocké, et ne prendre que les roaming DATA de d'utilisateur...

Dans la gestion des disques de profil utilisateur

Collection de sessions	
Afficher tout Général + Groupes d'utilisate + Disques de profi Session + Sécurité + Équilibrage de la c + Paramètres du clie + Disques de profil Implacement :	il utilisateur tilisateur permettent aux utilisateurs de stocker des paramètres et acement central. Vous pouvez activer la redirection de dossiers utilisateur dans une collection. Les serveurs de la collection intrôle total sur le partage du disque de profil utilisateur, et être membre du groupe Administrateurs local sur ce serveur. de profil utilisateur
\\dc-form\stock-up	rd-rds
I allie maximale (en	60) :
Il faut descendre dans les options et ne cocher que ce que l'on souhaite	Stocker seulement les dossiers suivants sur le disque de profil utilisateur Tous les autres dossiers du profil utilisateur ne seront pas conservés. Contacts Bureau Documents Téléchargements Liaisons Musique Images Données de profils utilisateur itinérants Données du Registre utilisateur
	Inclure les dossiers suivants :
Dans ce scenario le dossier appdata\local sera exclut.	Chemin d'accès Type Ajouter Supprimer
N.B: Si le profil doit intégrer un écran de démarrage, les infos étant stockées dans le fichier fichierappsFolder.itemdata-ms du dossier AppData\Local\Microsoft\Wind ows	Ajouter un fichier ou un dossier emplacement à inclure : ia\Local\microsoft\Windows chemin d'accès : Dossier Eichier Is les fichiers et les dossiers contenus dans un profil utilisateur peuvent inclus ou us.
On peut alors rajouter le dossier	<u>O</u> K <u>Annuler</u>
AppData\Local\Microsoft\Windows uniq	uement
Et voila Données de profils utilisateur itinérants Données du Registre utilisateur	
Inclure les dossiers suivants :	
Chemin d'accès Type \Appdata\Local\microsoft\Windows Dossier	Ajouter
< III	>



OK

Annuler

Appliquer

APPLICATIONS ET REMOTE APP

Objectif des applications distantes Remote App :

Les applications **Remote App** seront accessibles avec 2 techniques

• Soit via un Portail WEB avec une adresse spécifique

Le Portail Web aura une adresse du genre http://nom-srv/RDWeb et est accessible via tout intranet avec comme nom du serveur un FQDN.

Il s'agit de donner l'accès aux applications installées sur le serveur RDSH sans passer par le **bureau à distance**. On envois via le **protocole RDP** uniquement l'application, sans construire tout le bureau à distance. C''est très simple pour l'utilisateur, qui ne se mélange plus les idées entre son bureau "normal" et son "bureau à distance"...

Ce mode ne fonctionne qu'avec les **clients RPD 6.0** minimum et **Internet Explorer** car on utilise un **ActiveX**. L'objectif est de faire en sorte que les applications distances, (c'est-à-dire exécutées sur le Serveur RDS) se comporte au niveau du lancement très fortement comme des applications locales...Plusieurs applications peuvent être démarrées dans une session de type **Remote App**, chacune dans sa propre fenêtre.... De cette manière on rend transparent

- L'établissement de la connexion au serveur RDS
- o La redirection des ressources locales vers le serveur RDS
- Soit en les distribuant sur les clients, cette distribution pouvant se faire de 2 manières
 - o sous forme de fichier **.RDP**

On génère ces fichiers sur le serveur RDS et on les pose ensuite sur le bureau des clients... On effectue un clic droit sur une **Remote App** et on stocke ces fichiers dans un dossier partagé, on crée des raccourcis sur le Client.

NB: dans ce cas les associations de fichiers ne sont pas gérées

o sous forme de package MSI...

Que l'on peut déployer classiquement par stratégies. Abandonée !

Publication d'application Remote App :

Une fois l'application installée sur le **serveur RDSH** (cf chapitre précédent), elle doit être publiée dans la collection via **Taches / Publier des programmes Remote App**

Vue d'ensemble	PROGRAMMES REMOTEAPP Dernière actualisation le 23/05/2016	5 09:44:23 P	rogrammes Rem	. TÂCH	HES 🔻		↓
Collections	Filtrer	Q		-	Publier d Annuler	les progran la publicati	nmes RemoteApp on des programmes RemoteApp
formation RDS 2012	Nom du programme RemoteApp	Alias	Visible dans l'Ad	cès We	b des ser		
	Calculatrice	Calculatrice	Oui				
	Paint	Paint	Oui				
	WordPad	WordPad	Oui				



Un assistant se déclenche et liste les applications disponibles



On choisit ce que l'on veut publier, on vérifie est

)	Publier des programmes	RemoteApp 📃 🗖
Confirmation		
Programmes RemoteApp	Vérifiez que la liste des programmes Re	moteApp à publier est correcte puis cliquez sur Publier
Programmes RemoteApp Confirmation	Vérifiez que la liste des programmes Re 1 programme RemoteApp :	moteApp à publier est correcte puis cliquez sur Publier
Programmes RemoteApp Confirmation Publication	Vérifiez que la liste des programmes Re 1 programme RemoteApp : Programme RemoteApp	moteApp à publier est correcte puis cliquez sur Publier. Emplacement

C'est terminé

à	Publier des programmes Re	emoteApp	¢
Dernière étape			
Programmes RemoteApp	Les programmes RemoteApp sélectionnés formation RDS 2012.	ont été publiés correctement pour la collection	
Publication	1 programme RemoteApp a été publié po	ur la collection formation RDS 2012.	
Dernière étape	Programme RemoteApp	Statut	
	Microsoft Word 2010	Publié	

Notre Remote App est disponible

Vue d'ensemble	PROGRAMMES REMOTEAPP	C 15 20 40 L D		n []	Âcurs 📼
Serveurs	Derniere actualisation le 23/05/201	0 T5:29:48 P	rogramm	es Kem	ACHES *
Collections	Filtrer	Q			\odot
formation RDS 2012					
	Nom du programme RemoteApp	Alias	Visible	dans l'Accès	Web des ser
	Calculatrice	Calculatrice	Oui		
	Microsoft Word 2010	WINWORD	Oui		

Distribution d'application Remote App publiée:

Une application **RemoteApp**, correspondant donc à une application installée sur un serveur **RDSH** et **publiée**, doit encore être **distribuée** sur le client pour être utilisée.

2 méthodes principales existent pour la distribution :

- Portail WEB serveur RDWA
- Fichiers RDP connection distances client windows.

Une variante consiste à utiliser l'application Bureau à distance sur le Windows store



DISTRIBUTION PORTAIL RDWA

Groupe utilisateur du Bureau à distance (Vérification) :

Pour que les utilisateurs puissent se connecter aux applications Web, il faut ajouter les comptes au groupe local Utilisateurs du Bureau à distance

Cela est demandé dans l'assistant ajout de rôle RDSH, et normalement c'est déjà effectué, car on a testé la connexion, mais cela peut se compléter à tout moment.

On vérifier que le groupe Utilisateur du domaine soit incorporé dans le groupe local du serveur RDS nommé Utilisateurs du Bureau à distance.

Proprie	étés de : Utilisateurs du Bureau à distance	?	x			
Général						
Utilisateurs du Bureau à distance						
Description : Les membres de ce groupe disposent des droits nécessaires pour ouvrir une session à distance						
Membres :						
& FORM\Admins du domaine & FORM\Utilisateurs-RDS						

Ajout Serveur RDS au Groupe Ordinateurs Serveur RDS endpoint (Vérification):

il existe sur le serveur RDS Hôte de la session bureau a distance, un groupe local nommé Serveur RDS Endpoint

⊿ (擾 Utilisateurs et groupes l	Willisateurs de l'Analyseur de performances	Les membres de ce groupe peuvent accéder aux don
	Utilisateurs	Willisateurs de gestion à distance	Les membres de ce groupe peureix accès aux ressources
	Groupes	Mutilisateurs avec pouvoir	Les utilisateurs avec pouvoir sont inclus pour des rai
Þ 🕚	Performance	Mutilisateurs	Les utilisateurs ne peuvent pas effectuer de modifica
a= ¹	Gestionnaire de périphé	Serveurs RDS Endpoint	Les serveurs de ce groupe exécutent des ordinateurs
<u>ن</u>	Stockage	A Serveurs Gestion RDS	Les serveurs de ce groupe peuvent effectuer des acti
	Gestion des disques	🜆 Serveurs Accès Distant RDS	Les serveurs de ce groupe permettent aux utilisateur

Il faut que dans ce Groupe figure le compte ordinateur du serveur hébergeant l'accès WEB, (que cela soit le même serveur que le serveur Hôte des services RDS ou non)

Autrement dit le serveur qui héberge le RDWA doit faire partie du groupe Serveur RDS endpoint

	Pr	opriétés de : Serveurs RDS Endpoint	?	×
Général				
	Serveurs	s RDS Endpoint		
Descript	tion :	Les serveurs de ce groupe exécutent des ordinateurs hébergent des sessions où les utilisateurs, les progran	virtuels et nmes	
Membre	s :			
& AU				

N.B: si on ajoute une passerelle ultérieurement, il faudra penser à ajouter son compte ordinateur dans le groupe Serveur RDS Endpoint...


1° connexion Accès WEB https://UNCxxx/RDWEB :

Le nom du portail **Remote App** est du genre https://xxxUNCxxx/RDWEB donc https://rds-form.form.edu/RDWeb





Les service RDS WEB demandant d'installer automatiquement un **ActiveX**... il faut accepter... la 1° fois. (ensuite cela ne sera évidemment plus nécessaire)

On s'authentifie sur le portail (avec un compte autorisé à utiliser RDP...)



RDS 2012 R2 – accès intranet

- SYS 32 - Cours TP - ver 1.3 -



http://www.cabare.net Page 73 - Michel Cabaré -

Message Serveur de publication inconnu

Si on essaye de lancer une application on peut avoir encore un message comme quoi le serveur de publication est inconnue, mais si on demande la connexion quand même cela marche

5	RemoteApp				
Un site Web essaie d'exécuter un programme RemoteApp. L'éditeur de ce programme RemoteApp ne peut pas être identifié.					
Ce programme RemoteApp peut endommager votre ordinateur local ou distant. Ne vous connectez pas pour l'exécuter, sauf si vous en connaissez l'origine ou si vous l'avez déjà utilisé.					
	Éditeur :	Serveur de publication	inconnu		
<u> </u>	Type :	Programme RemoteApp			
	Chemin d'accès :	WINWORD			
	Nom :	Microsoft Word 2010			
	Ordinateur distant :	RDS-FORM.FORM.EDU			
Autoriser l'accès de l'ordinateur distant aux ressources suivantes de mon ordinateur : Lecteurs Presse-papiers Autres périphériques PnP pris en charge Imprimantes Enregistrement audio Les modifications apportées à ces options s'appliquent uniquement à cette connexion. Utiliser les informations d'identification suivantes pour la connexion : Mot de passe de bob@form edu					
(📥 Maso	quer détails		Connexion Annuler		

Il reste quelques inconvénients "ergonomiques"

- ✓ Message d'erreur de Certificats (connexion https)
- ✓ Double Authentification (on demande deux fois de se logguer)

on peut donc dire qu'il reste à gérer:

- les Certificats PKI
- La Double authentification en entrée sur le Portail puis sur le serveur RDS • gérant le Bureau à distance, c'est le SSO



DISTRIBUTION FICHIERS RDP

Déploiements applications RemoteApp et .RDP:

Pour générer un **.RDP** sous 2012 c'est très différent de sous 2008R2 ou il suffisait de faire un clic/droit sur le Serveur RDS 2008 pour l'application pour laquelle on voulait créer le .RDP

Programmes RemoteApp					
Nom			Chemin d'accès	Accès Burea	Arguments
Wicrosoft Word 2010		Ajo	uter des programmes RemoteApp	0	Désactivé
	Africa Africa Africa Ma		cher dans l'accès Bureau à distance quer dans l'accès Bureau à distance	e par le Web e par le Web	
-	∂	Cré Cré	er le fichier .rdp er le package Windows Installer		

N.B : avant d'executer cette procédure il est necessaire d'importer le certificat SSL du portal RDWA sur le client

Installation du certificat du portail WEB sur le client :

RDS 2012 R2 – accès intranet

- SYS 32 - Cours TP - ver 1.3 -

Pour récupérer le Certificat du portail Web il suffit de se connecter dessus, et on constate après le message l'erreur de certificat





http://www.cabare.net Page 75 - Michel Cabaré -

Assistant Importation de ceruncat	
Cet Assista de certificas o certificats o	enue ! Int vous aide à copier des certificats, des listes Its de confiance et des listes de révocation des depuis votre disque vers un magasin de
On va placer le c comme Autorités certification racine confiance	Assistant Importation de certificat × Assistant Importation de certificat × Agasin de certificats × S de Magasin de certificats sont des zones système où les certificats sont stockés. Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier l'emplacement du certificat. × Sélectionner automatiquement le magasin de certificats selon le type de certificat × Placer tous les certificats dans le magasin suivant ×
Sélectionner un magasin de certifica Sélectionnez le magasin de certificats qu voulez utiliser.	ats X Magasin de cettificats :
Personnel Autorités de certification racines Confiance de l'entreprise Autorités de certification intermé Éditeurs approuvés Certificats non autorisés Afficher les magasins physiques OK	de confi idiaires Placer tous les certificats dans le magasin suivant Magasin de certificats : Autorités de certification racines de confiance Parcourir Annuler
Et on valide et on cor	nfirme
Assistant Importation de d	Fin de l'Assistant Importation de certificat Ce certificat Ce certificat sera importé après que vous aurez cliqué sur Terminer. Vous avez spécifié les paramètres suivants : Magasin de certificats sélectionné par l'utilisateur Autor Contenu Contenu

On peut vérifier que le certificat est bien importé par le réaffichage du site WEB portail, il n'y a plus de message d'erreur :

RDS 2012 R2 – accès intranet

– SYS 32 – Cours TP - ver 1.3 -





http://www.cabare.net Page 76 - Michel Cabaré -

Paramétrage des connexions distantes du client windows :

Il faut aller dans le **panneau de configuration** et demande un affichage par petites icones, puis **Connexions RemoteApp et Bureau à distance** Ou plus simplement **Connexions distantes**

🕞 Connevions RemoteAnn et Rureau à	Connexions distantes	🍇 Con
	Emplacement Connexions distantes Gérez vos connexion Gérez vos connexion Gestionnaire d <mark>Bureau à distance</mark>	; RemoteApp et
On lance		



On rentre l'adresse du portail avec

https://rds-form.form.edu/RDWeb/Feed/webfeed.aspx



On continue l'assistant

Configurer (une nouvelle connexion avec les connexions RemoteApp et Bureau à distanceX igurer une nouvelle connexion avec les connexions RemoteApp et Bureau à distance
Prêt à co	onfigurer la connexion
URL de	connexion : https://rds-form.form.edu/RDWeb/Feed/webfeed.aspx
Window connexi	rs est prêt à ajouter les ressources disponibles (programmes et bureaux) de cette on à cet ordinateur. Cliquez sur « Suivant » pour continuer.
۲	Si vous continuez, des liens vers des programmes, des fichiers et des ordinateurs distants seront téléchargés et ajoutés à votre ordinateur. Ces liens seront mis à jour régulièrement et automatiquement à partir de l'URL de connexion. Ne continuez que si vous reconnaissez l'URL de connexion ci- dessus et que vous en connaissez la provenance.

Qui après authentification déclare qu'il a terminé..





Noter que la mise à jour est gérable assez automatiquement !



Récupération des fichiers .rdp :

Pour voir les raccourcis sur les RDP on demande afficher les ressources

Se connecter à des bureaux et programmes de votre espace de travail

Work Resources		Propriétés		
Cette connexion contient :	4 programmes et 0 bureaux Pour utiliser cette connexion, cl Tous les programmes, puis sur	Afficher les ressources liquez sur Démarrer, sur Connexions RemoteApp		
	et Bureau à distance.			
C:\Users\/	Administrateur \ AppData \ Roamir	ng\Microsoft\Windows\Start Menu\Program	s\Connexions Remote	
Etat de la 🛛 🌀 🖓 🐌	▼ Programmes ▼ Connexions Rem	noteApp et Bureau à distance 🔻 Work Resources	👻 🛂 Recherch	ner dans : Work
Dernière mit Fichier Edition	n Affichage Outils ?			
Organiser 🔻	Inclure dans la bibliothèque 🔻	Partager avec 🔻 Graver Nouveau dossier	r	-
🛛 🛨 🛨 🗄		Nom *	Modifié le	Туре
Date de cré	-	 Calculatrice (Work Resources) Microsoft Word 2010 (Work Resources) 	23/05/2016 17:47 23/05/2016 17:47	Raccourci Raccourci
	ieques	al Doint (Mark Dasauross)	22/05/2016 17:47	Daccourci





RDS 2012 R2 – accès intranet http://www.cabare.net Page 78

- Michel Cabaré -

N.B : pour les copier on fera clic droit ouvrir l'emplacement du fichier

📓 Calculatrice (Work Resources)	23/05/2016 17:47 Raccourci
🃅 Microsoft Word 2010 (Work Resource	es) 23/05/2016 17:47 Raccourci
<i>刻</i> Paint (Work Resources)	Exécuter avec le processeur graphique
🔊 WordPad (Work Resources)	Ouvrir l'emplacement du fichier

Pour éviter de saisir le chemin à la main...

C:\Users\Administrateur\AppData\Roaming\Microsoft\Workspaces\{6E1C18BD-6964-4197-BE20-617C31571							
🚱 🕞 🕨 🗛 Resource 🔹 🕼 Rechercher dans : Resource 💿 🗸 🚱 Rechercher dans : Resource							
Fichier Edition Affichage Outils ?	Fichier Edition Affichage Outils ?						
Organiser 🔻 👆 Connexion 🔻 Graver N	Nouveau dossier		· ·				
Documents	Nom ^	Modifié le	Туре				
S Images	🌄 Calculatrice (Work Resources).rdp	23/05/2016 17:47	Connexion Bureau				
S. Vidéos	Sicrosoft Word 2010 (Work Resources).rdp	23/05/2016 17:47	Connexion Bureau				
🚴 Administrateur	🌄 Paint (Work Resources).rdp	23/05/2016 17:47	Connexion Bureau				
Nordinateur	🌄 WordPad (Work Resources).rdp	23/05/2016 17:47	Connexion Bureau				

Utiliser les connexions distantes depuis windows 8.1 :

Soit des connexions remoteApp paramétrées



Le lancement est intégré dans le menu Tuiles Windows 8.1 dans une catégorie Work ressources RADC





RDS 2012 R2 – accès intranet - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 79 - Michel Cabaré - On peut décider si on le souhaite de poser les raccourcis correspondant sur le Bureau, mais ce n'est pas natif

Data	^ Nom	^	Modifié le	Туре	Taille
al	🗟 Calcul	atrice (Work Resources)	27/05/2016 12:01	Raccourci	4 Ke
alLow	Micro:	soft Excel 2010 (Work Resources)	27/05/2016 12:01	Raccourci	4 K
iming	Micros	soft Word 2010 (Work Resources)	27/05/2016 12:01	Raccourci	4 K
dobe	🔊 🔊 🔊	(Work Resources)	27/05/2016 12:01	Raccourci	4 K
entities breOffice	🛃 WordF	Pad (Work Resources)	27/05/2016 12:01	Raccourci	4 K
Calculatrice Microsoft E (Work Resources) 2010 (Work	ixcel WordPad (R Resource	Work Paint (Work Microso es) Resources) 2010 Reso	oft Word (Work urces)		
			Work Resources		
lancement génè lessage que l'ac	ere pour l'i cès par le	nstant les mêmes e portail, Il reste	Work Resources	(RADC) ice (Work Resou	ırces)
lancement génè lessage que l'ac onc quelques inco	ere pour l'i cès par le onvénients	nstant les mêmes e portail, Il reste "ergonomiques"	Work Resources Calculatri	(RADC) ice (Work Resou : Excel 2010 (W	irces) . Nouveau
lancement génè essage que l'ac onc quelques incc ✓ Message (connexion h	ere pour l'i cès par le onvénients d'erreur ittps)	nstant les mêmes e portail, Il reste "ergonomiques" de Certificats	Work Resources Calculatri Microsoft	(RADC) ice (Work Resou : Excel 2010 (W : Word 2010 (W	Irces) . Nouveau
lancement génè essage que l'ac onc quelques incc ✓ Message (connexion h ✓ Double Auth	ere pour l'i cès par le onvénients d'erreur ittps) nentificatio	nstant les mêmes e portail, Il reste "ergonomiques" de Certificats n (on demande	Work Resources Calculatri	(RADC) ice (Work Resou : Excel 2010 (W. : Word 2010 (W.	irces) Nouveau Nouveau
lancement génè essage que l'ac onc quelques inco ✓ Message (connexion h ✓ Double Auth deux fois de s	ere pour l'i cès par le onvénients d'erreur attps) nentificatio se logguer)	nstant les mêmes e portail, Il reste "ergonomiques" de Certificats n (on demande	Work Resources Image: Calculate Image: Calculate </td <td>(RADC) ice (Work Resou Excel 2010 (W. Word 2010 (W. ork Resources)</td> <td>Irces) . Nouveau Nouveau Nouveau</td>	(RADC) ice (Work Resou Excel 2010 (W. Word 2010 (W. ork Resources)	Irces) . Nouveau Nouveau Nouveau

Utiliser les connexions distantes depuis windows 7 :

Le lancement est parfaitement intégré dans le menu **Démarrer** de **Windows 7**

démarrer / tous les programmes / Connexions RemoteApp et bureau à distance

le lancement génère pour l'instant les mêmes message que l'accès par le portail, Il reste donc quelques inconvénients "ergonomiques"

- Message d'erreur de Certificats (connexion https)
- Double Authentification (on demande deux fois de se logguer)

on peut donc dire qu'il reste à gérer:

- les Certificats PKI
- La Double authentification en entrée sur le Portail puis sur le serveur RDS gérant le Bureau à distance, c'est le SSO





Pré-requis navigateurs:

Avec un serveur Web IIS 2008R2 (version 8), il fallait obligatoirement Internet Explorer comme navigateur avec un téléchargement d'activeX. Avec un serveur Web IIS 2012R2 (version 8.5), la situation est plus nuancée :

Edge windows 10 (sans Activex)

Car le navigateur Edge ne récupère plus les Activex...



L'accès au portail fonctionne mais sans l'onglet bureau a distance car celuici est instancié par l'activex...





IE 10 et IE 11 + Activex sur windows 8.1

A priori Ok, mais Il peut être nécessaire de modifier les entêtes de IIS

Pour des raisons de compatibilités, si on utilise les deux navigateurs les plus récents IE pour accéder au portail RDWEB, les icônes des **Remotes App** n'apparaissent pas...

Ce bug gênant peut se solutionner directement sur IIS sir on est sur un serveur 2008R2 Sp1... il faut modifier l'entête Http sur Serveur Web RDWEB en indiquant d'interpréter les pages en tant que IE9....

donc sur le serveur qui héberge les **Remote Apps**, on demande dans les outils d'administration, le gestionnaire des services internet IIS

on se place sur le site par défaut RDWEB et on va chercher les **En-têtes de réponse HTTP**...



par défaut on devrait avoir une seule ligne ASP.NET...





Utilisez cette fonction pour configurer les en-têtes HTTP ajoutés aux réponses du serveur Web.

Powered-By ASP.NET Héritée UA-Compatible IE=9 Local
(-UA-Compatible IE=9 Local
ais il faut ajouter la deuxième
Modifier l'en-tete de reponse HTTP personnalise

Nom :	
X-UA-Compatible	
Valeur :	N
IE=9	13

et re-démarrer le serveur !

IE 9 + Activex Seven

L'accès au portail la première fois déclenche la demande d'installation d'active X. une fois l'installation effectuée



	Aide
1	Domaine\Nom d'utilisateur : bob@form.edu Mot de passe : •
	Sécurité (<u>afficher les explications</u>) Ceci est un ordinateur public ou partagé. Ceci est un ordinateur privé.

2 Onglets s'affichent

Un onglet remoteApp et bureaux

Un onglet Se connecter à un ordinateur distants (si activex)



	Accès Bureau à distance par le W
Work Resources Connexions aux programmes RemoteApp et aux services Bureau à distance	
RemoteApp et Bureaux Se connecter à un ordinateur distant	Aide Se déconnecter
Dossier actuel : /	
Calculatrice Microsoft Paint WordPad	
	b Accès Bureau à distance par le We
Work Resources Connexions aux programmes RemoteApp et aux services Bureau à distance	
RemoteApp et Bureaux Se connecter à un ordinateur distant	Aide Se déconnecter
RemoteApp et Bureaux Se connecter à un ordinateur distant	Aide Se déco
trez le nom de l'ordinateur distant auquel vous voulez vous connecter, spécifiez les options, puis cliquez	sur Connexion.
Options de connexion	
Se <u>c</u> onnecter à : travail-10	
Taille du Bu <u>r</u> eau à distance : Plein écran	

Permettant d'accéder à n'importe quel ordinateur ayant le bureau à distance de configurer

L'activex est le suivant dans msrdpWebAccess.dll

Options >> Connexion

Gérer les modules complémentaires					
Afficher et gérer les modules complémentaires	d'Internet Explorer				
Types de module complémentaire	Nom	Éditeur 🔶	État	Durée d	Temps
Barres d'outils et extensions	McAfee, Inc.				
P Moteurs de recherche	scriptproxy	McAfee, Inc.	Désactivé	(0,14 s)	(0,00 s)
Accélérateurs	Microsoft Corporation				
SProtection contre le tracking	MsRdpClientShell Class	Microsoft Corporation	Activé		
	Groove GFS Browser H	Microsoft Corporation	Désactivé		
Afficher :	Office Document Cache	Microsoft Corporation	Désactivé	(0,06 s)	(0,03 s)
Modules complémentaires actuellement chargés	Groove Folder Synchron	Microsoft Corporation	Désactivé		
MsRdpClientShell Class Microsoft Corporation					
Version : 6.1.7600.16385 Date du fichier : Plus d'informations	Type : Rechercher le	Contrôle ActiveX module complémentain	e à l'aide du	moteur de re	ec

Navigateurs autres que IE:

Quelques remarques génériques :

- Il faut savoir que comme l'ActiveX ne pourra pas être chargé (c'est une techno propriétaire microsoft) il ne sera pas possible d'avoir l'apparition de l'onglet Acces ordinateur Distant
- Pour la même raison le SSo ne pourra pas être réalisé

Il faudra aussi que le navigateur sache comment gérer les associations de fichier . rdp qu'il va trouver sur le portail



Firefox

L'accès au portail avec Firefox peut déclencher un problème de certificat



Il faut demander Avancé, puis ajouter une exception et Confirmer l'exception

		Ajout d'une exception de sécurité
1	La connexion n'est pas sécurisée	Vous êtes en train de passer outre la façon dont Firefox identifie ce site. Les banques, magasins et autres sites web publics légitimes ne vous demanderont pas de faire cela. Serveur Adresse : https://rds-form.form.edu/RDWeb Obtenir le certificat
	Les propriétaires de rds-form.form.edu ont mal configuré leur site web. Pour éviter que vos données ne soient dérobées, Firefox ne s'est pas connecté à ce site web. En savoir plus <u>Retour</u> Avancé Signaler les erreurs similaires pour aider Mozilla à identifier les sites mal configurés rds-form.form.edu utilise un certificat de sécurité invalide. Le certificat n'est pas sûr car il est auto-signé	Ce site essaie de s'identifier lui-même avec des informations invalides. Voir Identité inconnue Le certificat n'est pas sûr car il est impossible de vérifier qu'il ait été délivré par une autorité de confiance utilisant une signature sécurisée.
_	Code d'erreur : SEC_ERROR_UNKNOWN_ISSUER	Conserver cette exception de façon permanente Confirmer l'exception de sécurité Annuler

Et on accède au portail



Echier Édition Affichage Historique Marque-pages Qutils ?	<u>_ ×</u>
Accès Bureau à distance par le Web 🗴 🕂	
< 🛈 🔒 https://rds-form.form.edu/RDWeb/Pages/fr-FR/login.aspx?ReturnUrl=/RDWeb/P 🛛 C 🔍 Rechercher	+ ♠ 🛛 🗉
🙆 Les plus visités 🛞 Débuter avec Firefox 🛞 Galerie de composant 🛞 Sites suggérés	
A A A A A A A A A A A A A A A A A A A	
🐻 Accès Bure	au à distance par le Web
Work Resources Connexions aux programmes RemoteApp et aux services Bureau à distance	Aide
	\sim
Domaine\Nom d'utilisateur : Mot de passe :	

Après authentification, les **remoteApp** apparaissent, mais pas l'onglet **Se connecter à un ordinateur distants**

	is-iorm.iorm.edu/RDvveb/I	Pages/II-FR/Delault.aspx	e	Kechercher	¥	•	111	0
lus visités 🛞 Début	r avec Firefox Galerie	de composant 🛞 Sites suggé	rés					
					to 🔂	tès Bureau à (distance p	oar le Web
Wc	rk Resources							
	rk Resources rions aux programmes Re	emoteApp et aux services Burea	u à distance					
RemoteApp e	rk Resources ^{kions aux programmes Re} t Bureaux	5 emoteApp et aux services Burea	u à distance		Aide	Se de	éconne	ecter
RemoteApp e	rk Resources iions aux programmes Re t Bureaux	emoteApp et aux services Burea	u à distance		Aide	Se de	éconne	ecter
RemoteApp e	rk Resources itions aux programmes Re t Bureaux :/ 	SemoteApp et aux services Burea	u à distance		Aide	Se de	éconne	ecter

Encore faut-il la première fois savoir quoi faire avec la recherche de l'application devant interpréter les **.rdp**

Work Resources	S emoteApp et aux services Bureau à distance	Ouverture de cpub-WINWORD-QuickSessionCollection-CmsRdsh.rdp
RemoteApp et Bureaux	Ouverture de cpub-WINWORD-QuickSessionCollection-CmsRdsh.rdp <u>D</u> Vous avez chois d'ouvrir : cpub-WINWORD-QuickSessionCollection-CmsRdsh.rdp	vous avez chois is down : cpub-WINWORD-QuickSessionCollection-CmsRdsh.rdp qui est un fichier de type : rdp File
Dossier actuel : / Calculatrice Microsoft Word 2010 Paint	qui est un fichier de type : rdp File à partir de : https://rds-form.form.edu Que doit faire Firefox avec ce fichier ? Ouvrir avec Parcourir Enragistrer le fichier Joujours effectuer cette action pour ce type de fichier. OK	a partir de : https://rds-form.form.edu Que doit faire Firefox avec ce fichier ? © Quvrir avec Connexion Bureau à distance © Enregistrer le fichier © Ioujours effectuer cette action pour ce type de fichier. Les paramètres peuvent être modifiés en utilisant l'onglet Applications des options de Firefox. OK Annuler
	Choix d'une application externe Criganiser ▼ Nouveau dossier Speech System32 System32 System32 System32 System32 Mom ^ Mom ^	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓



RDS 2012 R2 – accès intranet – SYS 32 – Cours TP - ver 1.3 -

http://www.cabare.net Page 86 - Michel Cabaré -

Présentation et Agencement du portail:

On l'a déjà dit, une **collection de session RDS**, peut héberger 2 types de ressources à l'exclusion l'un de l'autre...:

• un Bureau à distance (par défaut)



 un ou des Programmes RemoteApp (3 par défaut dans la collection QuickSessionCollection)

PROGRAMMES REMOTEAPP Dernière actualisation le 24/05/2016	5 14:13:19 F	Programmes Remote TÂCHES	•
Filtrer	Q		•
Nom du programme RemoteApp	Alias	Visible dans l'Accès Web des ser	vice
Calculatrice	calc	Oui	
Paint	mspaint	Oui	
WordPad	wordpad	Oui	

N.B : une solution de contournement existe, il suffit de publier une **remote App** du **bureau à distance** et de la paramétrer par défaut pour aller chercher un poste précis donné...

Paramètres - propriétés Remote App :

Pour chaque remoteApp installée il est possible depuis un clic droit / modifier les propriétés de changer quelques paramètres

les plus importants sont:

Filtrer	Q		
•			<u> </u>
Nom du programme RemoteApp	Alias	Visib	le dans l'Accès Web des servic
Calculatrice	Calculatrice	Oui	
Microsoft Word 2010	WINWORD	Oui	Modifier les propriétés
Paint	Paint	Oui	

Général

Pour définir le **nom**, le **dossier d'appartenance** et si cette **remoteApp** est accessible ou non via le portail



b	Propriétés 📃 🗖	x
E Calculatrice (Collect Afficher tout Général – Paramètres + Affectation d'utilis + Association de typ +	Propriétés – • ction formation RDS 2012) Général Scholler Strate Scholler Strate Nom du programme RemoteApp : Calculatrice Alias : Calculatrice Calculatrice Scholler Strate Emplacement du programme RemoteApp : C:\Windows\system32\calc.exe Icône actuelle : Scholler Strate Afficher le programme RemoteApp dans Accès Web des services Bureau à distance Image: Strate Strate Oui O Non Entrez le nom du dossier dans lequel vous voulez que ce programme RemoteApp apparaisse sur le serveur d'Accès Web des services Bureau à distance. Si vous voulez que le programme RemoteApp n'apparaisse dans aucun dossier, laissez ce champ vide.	X
	Dossier du programme RemoteApp : test	

Affectation d'utilisateurs

Ροι	ur définir de	es auto	risations			
Þ			Propriétés 📃 🗖			
(Calculatrice	(Colle	ction formation RDS 2012)			
	Affic Général Paramètres Affectation d'uti Association de t	ther tout + lis – yp +	Affectation d'utilisateurs Les programmes RemoteApp peuvent être limités de façon à ce que seuls des utilisateurs et des groupes sélectionnés puissent voir l'icône lorsqu'ils se connectent à l'accès Web des services Bureau à distance.	^		
			Spécifiez les utilisateurs et les groupes qui doivent voir ce programme RemoteApp : Tous les utilisateurs et tous les groupes qui ont accès à cette collection Seuls les utilisateurs et les groupes spécifiés Utilisateurs et groupes : Ajouter Supprimer	Ш		

Association de types de fichiers





Affichage dans des Dossiers

On peut considérer que les 3 remote app par défaut fassent parties d'un groupe de Test, pour lequel tous les utilisateurs auront accès. On veut les associer dans un dossier **Test remoteApp**

	Dossier du programme RemoteApp :		
Þ	Test RemoteApp	•	
V	¢		

Ce qui donnerait

Work Resources Connexions aux programmes RemoteApp et aux services Bureau à distance
RemoteApp et Bureaux Se connecter à un ordinateur distant
Dossier actuel : /
Test RemoteApp
Work Resources Connexions aux programmes RemoteApp et aux services Bureau à distance
RemoteApp et Bureaux Se connecter à un ordinateur distant
Dossier actuel : /Test RemoteApp
Monter Calculatrice Paint WordPad



Création de bureau distants

il suffit de publier une **remote App** pour chaque **bureau à distance que Ion souhaite avoir,** et la paramétrer par défaut pour aller chercher un poste précis donné...

Sé	électionner les	s programmes RemoteApp	
	Programmes RemoteAp Confirmation	p Sélectionnez les programmes RemoteApp à ajouter un programme RemoteApp à la liste Les programmes RemoteApp sont remplis à	à publier dans la collection QuickSessionCollection. e, cliquez sur Ajouter. à partir de SRV-RDS1.CABARE-INTRA.NET.
	Publication	Programme RemoteApp	Emplacement
		Assistant Configuration de la sécu	%SYSTEMDRIVE%\Windows\system32\scw.exe
		Calculatrice	%SYSTEMDRIVE%\Windows\system32\calc.exe
		🗌 🖳 Configuration du système	%SYSTEMDRIVE%\Windows\system32\msconfi
		🔽 🌄 Connexion Bureau à distance	%SYSTEMDRIVE%\Windows\system32\mstsc.exe
		🗌 🎼 Défragmenter et optimiser les Vecl	%SYSTEMDRIVE%\Windows\system32\dfrgui.exe

Confirmation		
Programmes RemoteApp	Vérifiez que la liste des programmes Remot	eApp à publier est correcte puis cliquez sur Publier.
Confirmation	1 programme RemoteApp :	
Publication	Programme RemoteApp	Emplacement
	Connexion Bureau à distance	%SYSTEMDRIVE%\Windows\system32\mstsc.exe

Lorsque c'est fait, on obtient une **Remote app** que l'on va paramétrer

PROGRAMMES REMOTEAPP Dernière actualisation le 24/05/2016	5 14:46:09 Pr	rogrami	mes Remot TÂCHES 🔻
Filtrer	٩	•	
Nom du programme RemoteApp	Alias	Visibl	e dans l'Accès Web des servic
Calculatrice	Calculatrice	Oui	
Connexion Bureau à distance	mstsc	Oui	
Paint	Paint	Oui	Modifier les propriétés

un non ,un dossier de rangement

Dossier du programme	RemoteApp :
----------------------	-------------

privé

mais surtout les droits d'accès

Affi	icher tout			
Général	+	Affectation d'utilisateurs		
Paramètres	+			
Affectation d'utilis		Les programmes RemoteApp peuvent être limitês de façon à ce que seuls des utilisateurs et des groupes sélectionnés puissent voir l'icône lorsqu'ils se connectent à		
Association de	typ +	l'accès Web des services Bureau à distance.		
		Spécifiez les utilisateurs et les groupes qui doivent voir ce programme RemoteApp : O Tous les utilisateurs et tous les groupes qui ont accès à cette collection		
		Utilisateurs et groupes :		
		CABARE-INTRA\Admins du domaine	Ajouter	
			Supprimer	



RDS 2012 R2 – accès intranethttp://www.c- SYS 32 – Cours TP - ver 1.3 -- Michel Cabo

http://www.cabare.net Page 90 - Michel Cabaré -

Et des paramètres d'appel obligatoires N:nom-hote-fqdn



Pour obtenir un bureau à distance sur la machine voulue nom-hote-fqdn

RemoteApp et Bureaux		
Dossier actuel : /privé		
1	N	
Monter	Connexion poste principal	

Dans les remoteApp il faus avoir autant de publication que de machines que l'on souhaite atteindre

PROGRAMMES REMOTEAPP Dernière actualisation le 24/05/2016 15:03:35 Programmes Remot [
Filtrer	۹	• (1) •		
Nom du programme RemoteApp	Alias	Visible dans l'Ac		
Calculatrice	Calculatrice	Oui		
Connexion poste principal	mstsc	Oui		
Connexion serveur Hyper-V SRV-V	mstsc (1)	Oui		
Connexion serveur hyper-V SRV-V1	mstsc (2)	Oui		

RemoteApp et Bureaux





RDS 2012 R2 – accès intranet - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 91 - Michel Cabaré -

Changer le titre du portail

On veut changer le titre Work Resources

Ainsi que le texte dessous Connexions aux programmes RemoteApp....



Pour le titre

en powershell, avec une commande du genre

Get-rdworkspace –connectionbroker nomhote.fqdn

PS C:\Users\Administrateur.CABARE-INTRA> g	et-rdworkspace -connectionbroker srv-rds1.cabare-intra.net
WorkspaceID	WorkspaceName
srv-rds1.cabare-intra.net	Work Resources
Puis Set-rdworkspace -name « :sdfjl	kbmkfj » –connectionbroker nomhote.fqdn

Pour le commentaire,

ntra.net

Il faut se placer sur le serveur qui héberge le rôle RDWA et éditer le fichier RDWAStrings.xml

Accueil Partage Afficha	ge
🕘 🔻 🏦 🕌 « Windows 🕨 Weł	b ▶ RDWeb ▶ Pages ▶ fr-FR
鷆 Web	^ Nom
퉬 RDWeb	Default arms
App Data	Derault.aspx
· · · · · · · · · · · · · · · · · · ·	Desktops.aspx
JE Error	login aspy
🚡 Feed	
Ecodi onin	logoff.aspx
FeedLogin	password.aspx
🍌 Pages	
🕒 Ann Data	😇 rap-nelp.ntm
	RDWAStrings.xml
iin 🔐	towa cos
📕 fr-FR	WE LSWALCSS

Il faut changer la ligne string id="HeadingApplicationName"

	RDWAStrings.xml - Bloc-notes
Fie	chier Edition Format Affichage ?
<	<pre>?xml version="1.0"?></pre>
<	rdwastr:strings xmlns:rdwastr="urn:microsoft.com:rdwastrings">
	<string id="PageTitle">Accès Bureau à distance par le Web</string>
	<string id="NoScriptWarning"></string>
	L'accès Bureau à distance par le Web requiert l'utilisation de JScript. Ce navigateur We
	 br/>
	 br/>
	Pour savoir si votre navigateur prend en charge JScript, ou pour autoriser les scripts,
	<string id="HeadingRDWA">Accès Bureau à distance par le Web</string>
	<string id="HeadingApplicationName">Connexions aux services à distance Cabaré GAF Grenoble Alpes Formationk, <string id="Help">Aide</string></string>





Besoin de certificats :

Il nous faut des certificats pour les applications qui sont mises à disposition sur notre serveur RDS, pour éviter le message de non confiance au lancement ...

Que ce soit pour authentifier la connexion au portail web en HTTPS...



ou simplement pour authentifier le serveur hôte du Bureau à Distance (ici une Application Word)

		<u>د</u>	
9 p	In site Web veut exéc rogramme ne peut pas	cuter un programme RemoteApp. L'éditeur de ce s être identifié.	
tte con	nexion distante peut endo	mmager votre ordinateur local ou distant. Ne vous connectez	
, sauf	si vous connaissez l'origin	ne de cette connexion ou si vous l'avez déjà utilisée.	
	Éditeur :	Serveur de publication inconnu	
S	Type :	Connexion Bureau à distance	
	Ordinateur distant :	SRV-RDS.cabare-intra.net	
oriser l	l'accès de l'ordinateur dist	tant aux ressources suivantes de mon ordinateur :	
	Lecteurs	✓ Ports	
	Presse-papiers	Autres périphériques PnP pris en charge	
	Imprimantes		
Déta	ils		
Déta	oteApp	Connexion Annuler	
Déta Remi	oteApp	Connexion Annuler	
Déta Remi	is otcApp Un site Web year programme ne per	Connexion Annuler	се
Déta Reme	is oteApp Un site Web yeut programme ne peu	exécuter un programme RemoteApp. L'éditeur de ut pas être identifié.	се
Déta Remi	is oteApp Un site Web yeut programme ne per ramme RemoteApp p	exécuter un programme RemoteApp. L'éditeur de ut pas être identifié.	ce onnecte
Déta Rem 3	is oteApp Un site Web yeut programme ne peu ramme RemoteApp p r1'exécuter, sauf si ve	exécuter un programme RemoteApp. L'éditeur de ut pas être identifié. eut endommager votre ordinateur local ou distant. Ne vous o ous en connaissez l'origine ou si vous l'avez déjà utilisé.	ce onnecte
Déta Rem Prog s pou	is oteApp Un site Web yeut programme ne per ramme RemoteApp p r l'exécuter, sauf si vo Éditeur :	exécuter un programme RemoteApp. L'éditeur de ut pas être identifié. eut endommager votre ordinateur local ou distant. Ne vous c ous en connaissez l'origine ou si vous l'avez déjà utilisé.	ce onnecte
Déta Reme Deta Spou	is oteApp Un site Web yeut programme ne pes ramme RemoteApp p r l'exécuter, sauf si vo Éditeur : Type :	Connexion Annuler Annuler Exécuter un programme RemoteApp. L'éditeur de tras être identifié. eut endommager votre ordinateur local ou distant. Ne vous c ous en connaissez l'origine ou si vous l'avez déjà utilisé. Serveur de publication inconnu Programme RemoteApp	ce onnecte
Déta Remo S prog s pou	is oteApp Un site Web yeut programme ne per ramme RemoteApp p r l'exécuter, sauf si vo Éditeur : Type : Chemin d'accès :	Connexion Annuler A	ce onnecte
Déta Remi 3	is oteApp Un site Web yeut programme ne per ramme RemoteApp pir l'exécuter, sauf si vi Éditeur : Type : Chemin d'accès : Nom :	Connexion Annuler Annuler Connexion Annuler Annuler Annuler Connexion Annuler Annuler Connexion Connexion Connexion Connexion Connexi	ce onnecte



Types de Certificats et PKI

Le Certificat sert à être sûr que la machine que l'on utilise soit la bonne.

Il existe 3 types de certificats SSL selon qu'ils soient émis par

- Autosigné (interne): la machine génère son propre certificat, qui n'est valable que sur... cette machine ! (à éviter !)
- PKI-de-domaine (interne): le certificat est valable sur tout le domaine (il suffit d'être sur une machine membre du domaine pour en bénéficier) (pour les tests, formations, c'est ok)
- PKI-internet (publique): le certificat est valable dans le monde entier. On peut en trouver des gratuits mais en général le service est payant(*) (obligatoire en production)

(*) **STARTSSL** propose des certificats gratuits fonctionnant sur 90 % des browser, **RAPIDSSL** propose des certificats connus par quasiment 100% des navigateurs pour environ 40€/an... ensuite il y a **Verisign.**. etc...

Les **PKI = PUBLIC KEY INFRASTRUCTURE** contiennent les clés publiques et privées permettant la reconnaissance et le cryptage= ETAT

Les PKI sont elles-mêmes émises, renouvelées et éventuellement révoquées,

elles sont construites selon une structure pyramidale. Une **PKI** est une identité qui effectue 3 opérations, elle émet, révoque et renouvelle des **certificats**.

Le **Certificat** = Pièce d'identité. On peut comparer les certificats à des pièces d'identités, permettant de reconnaître des machines dans un domaine. La signature de la carte d'identité prouve que le document de l'état est officiel, la signature du certificat par la PKI fait de même



Certificat / Certificat / Certificat / Certificat / Certificat / Certificat

(Carte nationale identité / Carte nationale identité / Carte nationale identité)

1 pièce d'identité à 3 éléments : Nom – prénom		
	Durée de Validité	
	Signature de l'Autorité = Etat / Préfecture	
1 certificat à 3 éléments :	Nom de poste/serveur en FQDN	
	Validité Horodatage	
	Origine de l'autorité de Certification = PKI	



Déroulement gestion des certificats:

On va opérer le déroulement suivant:

- 1. On monte une PKI de domaine (formation) sur le DC
- 2. puis il faudra certifier/signer le serveur **WEB IIS** pour valider **HTTPS**... c'est à dire faire une demande de certificat pour le serveur WEB, et l'appliquer
- puis il faudra certifier/signer le Serveur RDS c'est à dire faire une demande de certificat pour le Serveur RDS, et l'appliquer
 Si on monte un 2° Serveur RDS, une Gateway ou un Session Brooker il faut faire un demande de certificat pour chacun et les appliquer
- 4. puis il faudra valider/signer aussi chaque application publiée.

N.B: Si on monte les certificats avant d'installer les applications, elles seront automatiquement signées. Sinon il faut les re-signer.

Création PKI de domaine:

Si cela n'est pas fait, on crée une PKI de Domaine, connue dans toute l'AD.

La **PKI** se pose sur un serveur unique (pas de redondance possible) que l'on doit par conséquent sauvegarder. Il faut absolument ne pas la perdre !

On peut la stocker sur le **DC** qui intègre les **5 rôles**, et un **CG**. Lorsque l'on sauvera le **System State**, ou l'**AD**, elle fera partie de la sauvegarde...

Ajout rôle Service de certificats AD

Le rôle peut se poser sur un **DC** ou un serveur spécifique (...) mais jamais sur le <u>Serveur **RDS**</u>. C'est le rôle nommé **Services de certificats Active Directory**

Sélectionner des	s rôles de serv	eurs	SERVEUR DE DESTINATION dc-form.form.edu
Avant de commencer	Sélectionnez un ou	plusieurs rôles à installer sur le serveur sé	lectionné.
Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD CS Services de rôle Confirmation Résultats	Rôles ✓ Serveur DN: Serveur Wel ✓ Services AD Services AD Services AD Services AD Services AD Services Bur Services d'a Services d'a Services de ✓ Services de	S (Installé) b (IIS) DS (Installé) FS (Active Directory Federation Servic LDS (Active Directory Lightweight Dire RMS (Active Directory Rights Manage reau à distance (1 sur 6 installé(s)) ctivation en volume mpression et de numérisation de docu certificats Active Directory	Description Les services de certificats Active Directory (AD CS) servent à créer de autorités de certification et les services de rôle associés pour émettre et gérer les certificats utilisés dans diverses applications.
t toutes les	fonctions	Assistant Ajout de rôles	et de fonctionnalités X quises pour Services de
ssociées		certificats Active Directory ? Les outils suivants sont requis pour la fonctionnalité, mais ils ne doivent pas sur le même serveur.	a gestion de cette s obligatoirement être installés
		 Outils d'administration de server Outils d'administration de rô Outils des services de cer IOutils Outils Outils de gest 	ur distant les tificats Active Directory ion de l'autorité de certification



On est informé que les noms de poste et de domaine seront immuables...

a	Assistant Ajout de rôles et de fonctionnalités	_ _ X
Services de certif	icats Active Directory	SERVEUR DE DESTINATION dc-form.form.edu
Avant de commencer Type d'installation	Les services de certificats Active Directory (AD CS) fournissent l'inf en charge des scénarios tels que les réseaux sans fil sécurisés, les IPSec (Internet Protocol Security), la protection d'accès réseau (NA	irastructure de certificats pour prendre réseaux privés virtuels, la sécurité AP), le système de fichiers EFS
Sélection du serveur	(Encrypting File System) et la connexion par carte à puce.	
Rôles de serveurs	À noter :	
Fonctionnalités	 Les paramètres de nom et de domaine de cet ordinateur ne sor 	nt pas modifiables après l'installation
AD CS	d'une autorité de certification. Si vous voulez changer le nom d	e l'ordinateur, joindre un domaine ou
Services de rôle Confirmation	promouvoir ce serveur en controleur de domaine, effectuez ces l'autorité de certification. Pour plus d'informations, consultez Ai certification.	; modifications avant d'installer ttribution d'un nom à une autorité de

On demande uniquement Autorité de certification

	a	Assistant Ajout de rôles et de fonctionnalités	
	Sélectionner des s	services de rôle	SERVEUR DE DESTINATION dc-form.form.edu
On cor	Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD CS <u>Services de rôle</u> Confirmation	Sélectionner les services de rôle à installer pour Services de ce Services de rôle ✓ Autorité de certification □ Inscription de l'autorité de certification via le Web □ Répondeur en ligne □ Service d'inscription de périphérique réseau □ Service Web Inscription de certificats □ Service Web Stratégie d'inscription de certificats	ertificats Active Directory Description Une autorité de certification sert à émettre et gérer des certificats. Plusieurs autorités de certification peuvent être liées pour former une infrastructure à clé publique.
	a	Assistant Aiout de rôles et de fonctionnalités	
	Confirmer les séle	ctions d'installation	SERVEUR DE DESTINATION dc-form.form.edu
	Avant de commencer Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez Installer. Type d'installation Installer. Sélection du serveur Redémarrer automatiquement le serveur de destination, si nécessaire Rôles de serveurs Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées su cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités Fonctionnalités fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.		
	AD CS Services de rôle Confirmation Résultats	Outils d'administration de serveur distant Outils d'administration de rôles Outils des services de certificats Active Directory Outils de gestion de l'autorité de certification Services de certificats Active Directory	
		Autorité de certification	



RDS 2012 R2 – accès intranet - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 96 - Michel Cabaré -

Et cela s'installe

b	Assistant Ajout de rôles et de fonctionnalités
Progression de l'	installation Serveur de Destination de-form.form.edu
Avant de commencer	Afficher la progression de l'installation
Type d'installation	i Installation de fonctionnalité
Sélection du serveur	
Rôles de serveurs	Configuration requise. Installation réussie sur dc-form.form.edu.
Fonctionnalités	Services de certificats Active Directory
AD CS	Des étapes supplémentaires sont nécessaires pour la configuration des services de certificats
Services de rôle	Active Directory sur le serveur de destination. Configurer les services de certificats Active Directory sur le serveur de destination
Confirmation	Autorité de certification
Résultats	いていていていていていていていていていていていていていていていていていていて
	Outils d'administration de rôles
	Outils des services de certificats Active Directory
	Outils de gestion de l'autorité de certification

Paramétrage du rôle Service de certificats AD

Le Gestionnaire de Serveur nous indique qu'il reste à effectuer la configuration des services de certificat Active directory



Cela déclenche un assistant

2	Configuration des services de certificats Active Directory
Informations d'ic	entification dc-form.form.edu
Informations d'identificati Services de rôle Confirmation	. Spécifier les informations d'identification pour configurer les services de rôle
Progression Résultats	Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs local : • Utiliser l'autorité de certification autonome • Inscription de l'autorité de certification via le Web
	 Repondeur en ligne Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs d'entreprise : Autorité de certification d'entreprise Service Web Stratégie d'inscription de certificats Service Web Inscription de certificats Service Original d'entreprise
	Informations d'identification : FORM\Administrateur Modifier
	En savoir plus sur les rôles de serveur AD CS
	< Précédent Suivant > Configurer Annuler



RDS 2012 R2 – accès intranet - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 97 - Michel Cabaré -

Qui va configurer notre rôle Autorité de certification (il faut cocher)

B	Configuration des services de certificats Active Directory	_ _ ×
Services de rôle		SERVEUR DE DESTINATION dc-form.form.edu
Informations d'identificati	Sélectionner les services de rôle à configurer	
Services de rôle		
Type d'installation	✓ Autorité de certification	
Type d'AC	Inscription de l'autorité de certification via le Web	
Clé privée	Service d'inscription de périphériques réseau	
Chiffrement	Service Web Inscription de certificats	
Nom de l'AC	Service Web Stratégie d'inscription de certificats	
Période de validité		
Base de données de certi		
Confirmation		

De type entreprise (avec publication dans l'AD) la portée sera la forêt



On créé une PKI RACINE, (=équivalent ETAT) Dans certains cas on peut déclarer être une autorité de certification secondaire (=équivalent PREFECTURE)

è (Configuration des services de certificats Active Directory	
Type d'autorité de	e certification dc-form.form.edu	
Informations d'identificati	Spécifier le type de l'AC	
Services de rôle		
Type d'installation	Lorsque vous installez les services de certificats Active Directory (AD CS), vous créez ou étendez	
Type d'AC	une hiérarchie d'infrastructure à clé publique (PKI). Une autorité de certification racine se trouve au sommet de la hiérarchie PKI et émet ses propres certificats auto-signés. Une autorité de	
Clé privée	certification secondaire reçoit un certificat de l'autorité de certification de rang plus élevé dans la	
Chiffrement	hiérarchie PKI.	
Nom de l'AC	 Autorité de certification racine 	
Période de validité	Les autorités de certification racines sont les premières voire les seules autorités de certification	
Base de données de certi	computes dans due metachie PKI.	
Confirmation	 Autorité de certification secondaire 	
Progression	Les autorités de certification secondaires nécessitent une hiérarchie PKI établie et sont autorisées à émettre des certificats par l'autorité de certification de rang plus élevé dans la	
Résultats	hiérarchie.	



- SYS 32 - Cours TP - ver 1.3 -

RDS 2012 R2 – accès intranet http://www.cabare.net Page 98 - Michel Cabaré -

On demande de créer obligatoirement une nouvelle **clé privée**... sauf dans le cas d'une réinstallation, car <u>alors on utiliserait une clé déjà existante</u>...

N.B: Si lors d'une réinstallation on génère par erreur une nouvelle clé, il faudra refaire tous les certificats...

b	Configuration des services de certificats Active Directory		
Clé privée	SERVEUR DE DESTINATION dc-form.form.edu		
Informations d'identificati	Spécifier le type de la clé privée		
Services de rôle			
Type d'installation	Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une		
Type d'AC	clé privée.		
Clé privée	Créer une clé privée		
Chiffrement	Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.		
Nom de l'AC	○ Utiliser la clé privée existante		
Période de validité	Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de		
Base de données de certi	 Sélectionner un certificat et utiliser sa clé privée associée 		

On garde le chiffrement proposé RSA 2048 SHA1

b	Configuration des services de certificats Active Directory	_ □ X
Chiffrement pour	l'autorité de certification	SERVEUR DE DESTINATION dc-form.form.edu
Informations d'identificati	Spécifier les options de chiffrement	
Services de rôle		
Type d'installation	Sélectionnez un fournisseur de chiffrement :	Longueur de la clé :
Type d'AC	RSA#Microsoft Software Key Storage Provider	2048 🔻
Clé privée	Sélectionnez l'algorithme de hachage pour signer les certificats émis	par cette AC :
Chiffrement	SHA256	
Nom de l'AC	SHA384	
Période de validité	SHA512	
Base de données de certi	SHA1	
Confirmation	Autorisez l'interaction de l'administrateur lorsque l'autorité de cer	tification accède à la clé
Progression	privée.	ancadon accede a la cre

Le nom proposé par défaut peut être modifié, par exemple de **form-DC-FORM-CA** en **form-pki-CA** (pour **Certification Autorité pki** du domaine **FORM**)

b (Configuration des services de certificats Active Directory	_ D X
Nom de l'autorité	de certification	SERVEUR DE DESTINATION dc-form.form.edu
Informations d'identificati	Spécifier le nom de l'AC	
Services de rôle		
Type d'installation	Tapez un nom commun pour identifier cette autorité de certification	Ce nom est ajouté à tous les
Type d'AC	certificats emis par l'autorité de certification. Les valeurs des suffixes automatiquement, mais elles sont modifiables.	du nom unique sont générées
Clé privée		
Chiffrement	Nom commun de cette AC :	
Nom de l'AC	Torm-pki-CA	
Période de validité	Suffixe du nom unique :	
Base de données de certi	DC=form,DC=edu	
Confirmation	Apercu du nom unique :	
Progression	CN=form-pki-CA,DC=form,DC=edu	
Résultats		

Cela devient le nom de l'Autorité de Certification qui apparaîtra dans la console Services de Certificats Active Directory



On indique une durée de validité (on met la durée que l'on veut)



On garde les emplacements de stockage par défaut



Un résumé est affiché, on demande Configurer

B (Configuration des services de	e certificats Active Directory
Confirmation		SERVEUR DE DESTINATION dc-form.form.edu
Informations d'identificati	Pour configurer les rôles, service	s de rôle ou fonctionnalités ci-après, cliquez sur Configurer.
Services de rôle	 Services de certificats Acti 	ve Directory
Type d'AC	Autorité de certification Type d'AC :	Racine d'entreprise
Clé privée Chiffrement	Fournisseur de services de chiffrement :	RSA#Microsoft Software Key Storage Provider
Nom de l'AC	Algorithme de hachage : Longueur de la clé :	SHA1 2048
Base de données de certi	Autoriser l'interaction de l'administrateur :	Désactivé
Confirmation	Période de validité du certificat	24/05/2021 22:32:00
Progression Résultats	Nom unique : Emplacement de la base de données de certificats :	CN=form-pki-CA,DC=form,DC=edu C:\Windows\system32\CertLog
	Emplacement du journal de la base de données de certificats :	C:\Windows\system32\CertLog
		< Précédent Suivant > Configurer Annuler



RDS 2012 R2 – accès intranet - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 100 - Michel Cabaré -

Et on a une confirmation



Désormais une MMC nouvelle est disponible dans les Outils du **gestionnaire de** serveur...nommée Autorité de certification

Sur le Serveur ou on a installé l'autorité

nom de l'Autorité



Renouvellement PKI de domaine:

forcément cette PKi va arriver à échéance un jour

Gestionnaire de serveur (SRV-DC)	cabare-pki-CA (V0.0) Avertissement			
E P Roles	Nom	Statut	Date d'expiration	
	🗔 Certificat d'autorité de certific	ОК	23/04/2017 18:42	
 Berveal DNS Services Bureau à distance Services de certificats Active Directory 	🗐 🖈 Emplacement de AIA #1	OK	23/04/2017 18:42	
	🛛 🔏 Emplacement de CDP #1	Arrive à expiration	03/09/2013 16:56	
🗖 🙀 PKI d'entreprise	🔋 Emplacement de DeltaCRL #1	OK	04/09/2013 06:55	
cabare-pki-CA (V0.0)				
🚇 Modèl à de certificats				

il suffira alors de demander Toutes les tâches / Renouveler le Certificat d'autorité de certification

Gestionnaire de serveur (SR	(V-DC)	cabare-pki-CA			
 ➡ ■ Roles ● ■ Serveur DHCP ● ■ Services Bureau à d ■ ■ Services de certifica ■ ■ PKI d'entreprise ■ abare-pki-CA 	istance ts Active Directory IA (V0.0) ificats	Nom Certificats révoqués Certificats délivrés Demandes en attente Demandes ayant échoué Modèles de certificats			
📔 Certificats	Toutes les tâches 🔹 🕨	Démarrer le service			
🧮 Certificats 🛅 Demandes	Affichage 🕨 .	Arrêter le service			
🧮 Demandes	Actualiser	Soumettre une nouvelle demande			
i Modèles di i i i i i i i i i i i i i i i i i i	Exporter la liste	Sauvegarder l'autorité de certification			
	Propriétés .	Restaurer l'autorite de certification			
🖃 🚋 Diagnostics	Aide	Renouveler le certificat d'autorité de certification			



http://www.cabare.net Page 101 - Michel Cabaré -

un message apparaît

Installer un certificat d'autorité de certific Les services de certificats Active Directory ne p pendant cette opération. Voulez-vous arrêter le Active Directory maintenant ?	il ne faut pas renouveler les clés
	Renouveler le certificat d'autorité de certification
NON, car si on renouvelle les clés, il faudra refaire tous les certificats !	Outre l'obtention d'un nouveau certificat pour votre autorité de certification, vous pouvez aussi créer une nouvelle clé de signature. Vous avez besoin d'un nouveau certificat pour votre autorité de certification lorsque : Image: Construction d'un nouveau certificat que vous délivrez actuellement est limitée. Vous avez besoin d'une nouvelle clé de signature lorsque : Vous avez besoin d'une nouvelle clé de signature lorsque : Vous avez besoin d'une nouvelle clé de signature lorsque : Vous disposez d'un programme qui nécessite qu'une nouvelle clé de signature soit utilisée avec un nouveau certificat de l'autorité de certification. La liste de révocation des certificats actuelle est trop grande et vous voulez déplacer une partie de ses informations dans une nouvelle liste. Voulez-vous créer une nouvelle paire de clés publique et privée ? Les paramètres de fournisseur de services de chiffrement, de longueur de clé et d'algorithme de hachage servint e augmentée. Image: Dui Non

et on obtient le renouvellement



Voici quelques certificats types

Certificats délivrés									
ID de la demande	Nom du demandeur	Certificat binaire	Modèle de certificat	Numéro de série	Date d'effet du certificat				
2	CABARE-INTRA\SR	BEGIN CERT	Échange d'autorité de certification (CAExchange)	3b9294be00000	23/04/2012 18:33				
3	CABARE-INTRA\SR	BEGIN CERT	Contrôleur de domaine (DomainController)	3ba1161f00000	23/04/2012 18:49				
4	CABARE-INTRA\Ad	BEGIN CERT	Serveur Web (WebServer)	3bb41d2700000	23/04/2012 19:10				
5	CABARE-INTRA\SR	BEGIN CERT	Contrôleur de domaine (DomainController)	3c1604d000000	23/04/2012 20:57				
5 6	CABARE-INTRA\Ad	BEGIN CERT	Serveur Web (WebServer)	3e2cfbcd00000	24/04/2012 06:41				
7	CABARE-INTRA\SR	BEGIN CERT	Contrôleur de domaine (DomainController)	14b9e92b00000	17/10/2012 09:09				
I	CABARE-INTRA\SR	BEGIN CERT	Contrôleur de domaine (DomainController)	18ed905700000	13/03/2013 00:14				
1 1 1 1 1 1 1 1 1 1	CABARE-INTRA\SR	BEGIN CERT	Échange d'autorité de certification (CAExchange)	361ef22600000	02/09/2013 18:35				
11	CABARE-INTRA\Ad	BEGIN CERT	Serveur Web (WebServer)	362f566000010	02/09/2013 19:07				
12	CABARE-INTRA\SR	BEGIN CERT	Contrôleur de domaine (DomainController)	3d82dc3a00010	05/09/2013 13:28				



Déploiement - Quels Certificats pour Quels Serveurs:

On se met sur la Vue d'ensemble des Services Bureau à distance, et on demande dans les tâches de Modifier les propriétés du déploiement



Et on se place sur Certificats

à	Propriétés de déploiem	ent		_ □	x				
Configurer le déploiement									
Afficher tout Passerelle des serv + Gestionnaire de lic + Accès Web des ser + Certificats –	Gérer les certificats Un déploiement des services Bureau à distance requiert des certificats pour l'authentification du serveur, pour l'authentification unique et pour l'établissement de connexions sécurisées. Le niveau de certification actuel du déploiement est Non configuré								
	Service de rôle	Niveau	État	État					
	Service Broker pour les connexions	Non configuré							
	Service Broker pour les connexions	Non configuré							
	Accès Web des services Bureau à di	Non configuré			≡				
	Passerelle des services Bureau à dist	Inconnu							
	< 1	1		>					
	Nom de sujet : Non applicable Afficher les détails Ce certificat est requis pour l'authentif services Bureau à distance. Vous pouvez mettre à jour ce certificat certificat existant.	ication du serveur au t en créant un certific Sélection	uprès du dépl cat ou en séle	loiement des ectionnant un					

On l'a déjà dit, Pour <u>chaque serveur physique / rôle logique</u>, il faut faire une demande de **Certificat** pour attester que cette machine est bien celle qui porte ce nom là... (ne jamais renommer un Serveur, sans refaire le Certificat)

3 machines – rôles doivent être certifiés au minimum (4 si l'on a une passerelle)

 Sur le Serveur qui héberge le Rôle Hôte RDSH, il va falloir <u>effectuer une</u> demande de certificat avec le nom FDQN du serveur, puis l<u>'appliquer</u> au Serveur (rôle Broker pour l'authentification SSo)

Service de rôle	Niveau	État	État
Service Broker pour les connexions	Non configuré		
Service Broker pour les connexions	Non configuré		
Accès Web des services Bureau à di	Non configuré		
Passerelle des services Bureau à dist	Inconnu		
<		>	

Nom de sujet : Non applicable Afficher les détails

Ce certificat est requis pour l'authentification du serveur auprès du déploiement des services Bureau à distance.



• Sur le Serveur qui héberge le Rôle Hôte **RDSH**, il va falloir effectuer une demande de certificat avec le nom **FDQN** du serveur, puis l'appliquer au Serveur (**Rôle RDSH pour authentification application RemoteApp**)

N.B: Si un certificat existe déjà pour cette machine, il <u>suffit de</u> <u>l'appliquer</u> sans redemander la création.

Service de rôle	Niveau	État	État
Service Broker pour les connexions	Non configuré		
Service Broker pour les connexions	Non configuré		
Accès Web des services Bureau à di	Non configuré		
Passerelle des services Bureau à dist	Inconnu		
< 1	1		>

Nom de sujet : Non applicable Afficher les détails

Ce certificat est requis pour la signature des fichiers RDP afin d'éviter tout message d'avertissement supplémentaire pour l'utilisateur.

 Sur le Serveur qui héberge le Rôle Serveur RDWA, il va falloir effectuer une demande de certificat avec le nom FDQN du serveur, puis l'appliquer au serveur (Rôle RDWA pour https).

Service de rôle	Niveau	État	État
Service Broker pour les connexions	Non configuré		
Service Broker pour les connexions	Non configuré		
Accès Web des services Bureau à di	Non configuré		
Passerelle des services Bureau à dist	Inconnu		
< ۱	I		>

Nom de sujet : Non applicable Afficher les détails

Ce certificat est requis pour l'activation de l'abonnement à la connexion RemoteApp et Bureau à distance, ainsi que pour l'authentification serveur de l'accès Bureau à distance par le Web.

 Dans le cas d'une configuration avec une passerelle, il faudra également effectuer une demande de certificat avec le nom FDQN du serveur, puis l'appliquer sur la Gateway

Demande de création de Certificat de Domaine - via IIS:

Il faut donc d'abord se créer un **certificat de domaine**. Cela peut se faire pour notre Serveur **RDSH / RDWA** par la console **Gestionnaire IIS**

Dans le gestionnaire de Serveur on demande gestionnaire des services internet (IIS)



Dans la console, on se place sur notre serveur, puis dans la section **IIS** on clic sur **Certificats de serveur**





le certificat auto-signé du serveur apparaît

Connexions	Certif	ficats de serveur	
Page de démarrage RDS-FORM (FORM\Administr	Utilisez cette fond accéder aux sites	tion pour demander et gérer les certificats Web configurés pour le protocole SSL.	servant au serveur Web pour
	Filtrer :	🗸 💎 Atteindre 👒 🔙 Affiche	er tout Regrouper par :
	Nom	Délivré à	Émis par
		rds-form.form.edu	rds-form.form.edu

Pour avoir un certificat de domaine (la racine PKI étant déjà créé), il faut demander clicdroit Créer un certificat de domaine...

Certificats de serveur

Utilisez cette fonction pour demander et gérer les certificats servant au serveur Web pour accéder aux sites Web configurés pour le protocole SSL.



Seule la première ligne Nom commun avec le FQDN est importante

- SYS 32 - Cours TP - ver 1.3 -

	Créer un certificat
Propriétés du	ı nom unique
Indiquez les informations re ville/localité, utilisez des no Nom commun :	equises pour le certificat. Lorsque vous entrez le département ou région et la ms complets et officiels, et n'employez aucune abréviation. rds-form.form.edu
Organisation :	formation
Unité d'organisation :	informatique
Ville :	grenoble
Département/région :	isere
Pays/région :	FR v



RDS 2012 R2 – accès intranet http://www.cabare.net Page 105 - Michel Cabaré -

Ensuite il faut aller chercher notre autorité racine PKI par Sélectionner

	Créer un certificat		? X
P	Autorité de certification en ligne		
Indique il doit ê Indique	z l'autorité de certification de votre domaine qui signera le certificat. Un n rre facile à retenir. r une autorité de certification en ligne :	om convivial est	nécessaire ;
			Sélectionner
Exemple	: NomAutoritéCertification\NomServeur		
Nom co	nvivial :		

Et choisir notre **PKI**

	Sélectionner une autorité de certification						
Sélectionner l'autorité de certi	fication à utiliser :						
Autorité de certification	Ordinateur						
form-pki-CA dc-form.form.edu							

N.B: Dans Sélectionner... cela peut mettre du temps à apparaître, et on peut faire un gpupdate /force pour accéllerer un peu

C:\User: Mise à ,	s\Admin jour de	nistr e la	ate str	ur.CABARE- atégie	-INTRA≻gpupda	ate ∕fo	orce		
La mise	à jou	r de	la	stratégie	utilisateur	s'est	terminée	sans	erreur.
La mise	à jou	r de	la	stratégie	d'ordinateur	s'est	t terminée	sans	erreur.

Et on donne un nom pratique à retenir, par exemple certif-rdsh

Créer un certificat	? ×
Autorité de certification en ligne	
Indiquez l'autorité de certification de votre domaine qui signera le certificat. Un nom convivial est il doit être facile à retenir. Indiquer une autorité de certification en ligne :	t nécessaire ;
form-pki-CA\dc-form.form.edu	Sélectionner
Exemple : NomAutoritéCertification\NomServeur	
Nom convivial :	
certif-rdsh	

Et on notre certificat de domaine se crée, ici certif-rdsh

Certifi Certifi	cats de serveur	
Utilisez cette foncti accéder aux sites W	ion pour demander et gérer les certificats s Veb configurés pour le protocole SSL.	ervant au serveur Web pour
Filtrer :	🗸 🐺 Atteindre 👒 🕁 Afficher	tout Regrouper par : 💂
Nom	Délivré à	Émis par
	rds-form.form.edu	rds-form.form.edu
certif-rdsh	rds-form.form.edu	form-pki-CA
	Certifi Utilisez cette fonct accéder aux sites V Filtrer : Nom	Certificats de serveur Utilisez cette fonction pour demander et gérer les certificats s accéder aux sites Web configurés pour le protocole SSL. Filtrer :



RDS 2012 R2 - accès intranethttp://www.cabare.netPage 106- SYS 32 - Cours TP - ver 1.3 -- Michel Cabaré -

N.B : par mesure de sécurité, et pour éviter toute confusion, on peut supprimer le certificat auto signé et ne garder que celui de domaine !

Certifica	ats de serveur		
Utilisez cette fonctior accéder aux sites Web	n pour demander et gérer les cert o configurés pour le protocole SS	ificats servant au serveur Web pour L.	
Filtrer :	🗸 🐨 Atteindre 🕞 🐺 A	Afficher tout Regrouper par :	Ŧ
Nom	Délivré à	Émis par	
certif-rdsh	rds-form.form.edu	form-pki-CA	

A titre d'information notre certificat est présent sur le serveur ou est installé l'Autorité de certification, dans les certificats délivrés

ā.	certsrv - [Autorité d	e certification (Local)\for	rm-pki-CA\Certif	icats délivrés]
Fichier Action Affichage ?				
🗢 🄿 🖄 🙆 👔				
🙀 Autorité de certification (Local)	Unité d'organisation d'émission	Nom commun d'émission	Ville d'émission	Dépt / Région d'émissi
 ✓ J form-pki-CA Certificats révoqués Certificats délivrés Demandes en attente 	informatique	rds-form.form.edu	grenoble	iseère

Il correspond à un certificat garantissant un ordinateur, délivré par notre pki..

Export de certificat:

Toujours depuis la console IIS on va exporter ce certificat clic droit Exporter...

Certific Utilisez cette fonctio accéder aux sites We	ats de serveur n pour demander et gérer les certif b configurés pour le protocole SSL	ïcats servant au serveur Web pour
Filtrer :	- 🍸 Atteindre 🕞 🖓 Af	ficher tout Regrouper par :
Nom 📩	Délivré à	Émis par
certif-rdsh	rds-form.form.edr	Importer
		Créer une demande de certificat Terminer la demande de certificat
		Créer un certificat de domaine
		Créer un certificat auto-signé
		Afficher
		Exporter

En le plaçant à un endroit accessible,

par exemple un emplacement \\nas-1\commun\xxxx. pfx	Exporter vers : \\nas-1\commun\certificat\certif-rdsh.pfx
Et 1 mot de passe identique pour tous les certificats, du genre certifxxxx	Mot de passe : •••••••••• Confirmer le mot de passe : •••••••••



RDS 2012 R2 – accès intranet – SYS 32 – Cours TP - ver 1.3 -

http://www.cabare.net Page 107 - Michel Cabaré -

ОК

h

Exporter un certificat

? x

Annuler

Application / import de Certificat:

Dans la console **Configurer le Déploiement – Certificats** on n'utilise surtout pas **Créer un certificat** (qui crée des certificats auto signé) car on va aller chercher les certificats de domaine que l'on a préalablement crée via **IIS**.

On se place sur le premier Rôle et via Sélectionner un certificat existant

Service de rôle	Niveau	État	État
Service Broker pour les connexions	Non configuré		
Service Broker pour les connexions	Non configuré		
Accès Web des services Bureau à di	Non configuré		
Passerelle des services Bureau à dist	Inconnu		
<			
Iom de sujet : Non applicable	1		3
Nom de sujet : Non applicable Afficher les détails Ce certificat est requis pour l'authentifi ervices Bureau à distance.	ication du serveur au	ıprès du dép	loiement des
lom de sujet : Non applicable Afficher les détails Ce certificat est requis pour l'authentifi ervices Bureau à distance. /ous pouvez mettre à jour ce certificat ertificat existant.	ication du serveur au : en créant un certific	uprès du dép cat ou en sél	loiement des ectionnant un

On va chercher notre certificat précédemment exporté

Þ		Sélectionner un certificat	existant		
Vo à c	ous pouvez choisir d'appliquer le co distance ou bien vous pouvez sélec	ertificat qui est actuellement stocké sur le ctionner un autre certificat qui est stocké é	serveur du service Bi dans un fichier de cei	roker pour les (rtificat PKCS,	connexions Bure
C) Appliquer le certificat stocké sur Mot de passe :	le serveur du service Broker pour les conn	exions Bureau à dist	ance	
۲) Choisir un autre certificat				
	\\nas-1\commun\certificat\certif	f-rdsh.pfx			Darsourin
	Mot de passe :				Parcount
⊡ dem	Autoriser l'ajout du certificat au r destination Ande Appliquer	nagasin de certificats Autorités de certifica Un seul certificat peut être ajouté des certificats à des services de re OK.	ation racines de conf è à la fois à un service ôle supplémentaires,	iance sur les or e de rôle donné cliquez sur Ap	rdinateurs de é. Pour ajouter pliquer ou sur
dem	Autoriser l'ajout du certificat au r destination Ande Appliquer	 Magasin de certificats Autorités de certificat Un seul certificat peut être ajouté des certificats à des services de ré OK. Le niveau de certification actuel du di Qu'est-ce qu'un niveau de certification 	ation racines de conf à la fois à un service ôle supplémentaires, éploiement est Non n ?	iance sur les or e de rôle donné cliquez sur Ap configuré	é. Pour ajouter pliquer ou sur
dem	Autoriser l'ajout du certificat au r destination Ande Appliquer	 Magasin de certificats Autorités de certificat Un seul certificat peut être ajouté des certificats à des services de ré OK. Le niveau de certification actuel du di Qu'est-ce qu'un niveau de certification Service de rôle 	ation racines de conf à la fois à un service ôle supplémentaires, éploiement est Non on ? Niveau	iance sur les or e de rôle donné cliquez sur Ap configuré État	é. Pour ajouter pliquer ou sur État
dem	Autoriser l'ajout du certificat au r destination	 Magasin de certificats Autorités de certificat Un seul certificat peut être ajouté des certificats à des services de re OK. Le niveau de certification actuel du d Qu'est-ce qu'un niveau de certification Service de rôle Service Broker pour les connexions 	ation racines de conf à la fois à un service ôle supplémentaires, éploiement est Non on ? Niveau Non configuré	iance sur les or e de rôle donné cliquez sur Ap configuré État 	é. Pour ajouter pliquer ou sur État Prêt à app
dem	Autoriser l'ajout du certificat au r destination	 Magasin de certificats Autorités de certificat Un seul certificat peut être ajouté des certificats à des services de ré OK. Le niveau de certification actuel du di Qu'est-ce qu'un niveau de certification Service de rôle Service Broker pour les connexions Services Broker pour les connexions Accès Web des services Bureau à d 	ation racines de conf à la fois à un service ôle supplémentaires, éploiement est Non on ? Niveau Non configuré i Non configuré i Non configuré	iance sur les or e de rôle donné cliquez sur App configuré État 	é. Pour ajouter pliquer ou sur État Prêt à app
dem	Autoriser l'ajout du certificat au r destination	 Magasin de certificats Autorités de certificat Un seul certificat peut être ajouté des certificats à des services de ré OK. Le niveau de certification actuel du di Qu'est-ce qu'un niveau de certification Service de rôle Service Broker pour les connexions Service Broker pour les connexions Accès Web des services Bureau à di Passerelle des services Bureau à dis 	ation racines de conf à la fois à un service ôle supplémentaires, éploiement est Non on ? Niveau Non configuré Non configuré i Non configuré st Inconnu	iance sur les or e de rôle donné cliquez sur Ap configuré État 	é. Pour ajouter pliquer ou sur État Prêt à app
dem	Autoriser l'ajout du certificat au r destination	 Magasin de certificats Autorités de certificat Un seul certificat peut être ajouté des certificats à des services de ré OK. Le niveau de certification actuel du di Qu'est-ce qu'un niveau de certification Service de rôle Service Broker pour les connexions Service Broker pour les connexions Accès Web des services Bureau à dis < 	ation racines de conf à la fois à un service ôle supplémentaires, éploiement est Non on ? Niveau Non configuré Non configuré li Non configuré si Inconnu III	iance sur les or e de rôle donné cliquez sur App configuré État 	é. Pour ajouter pliquer ou sur État Prêt à app
dem	Autoriser l'ajout du certificat au r destination	 Magasin de certificats Autorités de certificat Un seul certificat peut être ajouté des certificats à des services de ro OK. Le niveau de certification actuel du d Qu'est-ce qu'un niveau de certification Service de rôle Service Broker pour les connexions Service Broker pour les connexions Accès Web des services Bureau à di Passerelle des services Bureau à dis C Nom de sujet : Non applicable Afficher les détails Ce certificat est requis pour l'authent services Bureau à distance. 	ation racines de conf à à la fois à un service à la fois à un service à la supplémentaires, éploiement est Non n? Niveau Non configuré Non configuré Inconnu iii iii iiii iiii Non configuré	iance sur les or e de rôle donné cliquez sur Ap configuré État 	é. Pour ajouter pliquer ou sur État Prêt à app >
dem	Autoriser l'ajout du certificat au r destination	 Magasin de certificats Autorités de certificat Un seul certificat peut être ajouté des certificats à des services de ro OK. Le niveau de certification actuel du di Qu'est-ce qu'un niveau de certification Service de rôle Service Broker pour les connexions Service Broker pour les connexions Accès Web des services Bureau à dis C Nom de sujet : Non applicable Afficher les détails Ce certificat est requis pour l'authent services Bureau à distance. Vous pouvez mettre à jour ce certification 	ation racines de conf à la fois à un service ble supplémentaires, éploiement est Non n? Niveau Non configuré Non configuré Non configuré I Non configuré I Non configuré ification du serveur a at en créant un certif	iance sur les or e de rôle donné cliquez sur App configuré État euprès du déple icat ou en sélev	ctionnant un


veau	Approuvé (certificat o	de domain	e) Etat (ЭK
	Gérer les certificats			
	Un déploiement des services Bureau à l'authentification du serveur, pour l'aut connexions sécurisées.	distance requiert d thentification uniqu	les certificats p ue et pour l'éta	oour blissement de
	Le niveau de certification actuel du dé Qu'est-ce qu'un niveau de certification	ploiement est Non 1 ?	configuré	É
	Le niveau de certification actuel du dé Qu'est-ce qu'un niveau de certification Service de rôle	ploiement est Non ? Niveau	État	État
	Le niveau de certification actuel du dé Qu'est-ce qu'un niveau de certification Service de rôle Service Broker pour les connexions	ploiement est Non ? Niveau Approuvé	configuré État OK	État Réussite
	Le niveau de certification actuel du dé Qu'est-ce qu'un niveau de certification Service de rôle Service Broker pour les connexions Service Broker pour les connexions	ploiement est Non ? Niveau Approuvé Non configuré	Configuré État OK 	État Réussite
,	Le niveau de certification actuel du dé Qu'est-ce qu'un niveau de certification Service de rôle Service Broker pour les connexions Service Broker pour les connexions Accès Web des services Bureau à di	ploiement est Non ? Niveau Approuvé Non configuré Non configuré	configuré État OK 	État Réussite
•	Le niveau de certification actuel du dé Qu'est-ce qu'un niveau de certification Service de rôle Service Broker pour les connexions Service Broker pour les connexions Accès Web des services Bureau à dis Passerelle des services Bureau à dist	ploiement est Non ? Niveau Approuvé Non configuré Non configuré Inconnu	configuré État OK 	État Réussite

<u>Comme les 3 rôles sont sur le même serveur</u>, on refait la manip 2 fois de manière à avoir au final les 3 certificats (pour le même serveur physique)

Gérer les certificats

Un déploiement des services Bureau à distance requiert des certificats pour l'authentification du serveur, pour l'authentification unique et pour l'établissement de connexions sécurisées.

Le niveau de certification actuel du déploiement est **Approuvé** Qu'est-ce qu'un niveau de certification ?

Service de rôle	Niveau	État	État
Service Broker pour les connexions	Approuvé	OK	Réussite
Service Broker pour les connexions	Approuvé	OK	Réussite
Accès Web des services Bureau à di	Approuvé	OK	Réussite
Passerelle des services Bureau à dist	Inconnu		
۲ ا	11		>

Application du Certificat sur IIS pour SSL (vérification) :

- SYS 32 - Cours TP - ver 1.3 -

Dans le Gestionnaire IIS on demande dans les Sites, sur le Site Web par défaut Default Web Site et clic droit Modifier les liaisons...





Et la on sélectionne ensuite la liaison https 443, et en demandant Modifier...

	? X				
Туре	Nom de l'hôte	Port	Adresse IP	Informations sur	Aiouter
http		80	*		
https		443	*		Modifier

Si besoin on indique le nom "pratique" du certificat de domaine

Modifier la liaison	de site ? X
Type : Adresse IP : https V Toutes non attribuées Nom de l'hôte :	Port :
Exiger l'indication de nom du serveur	
Certificat SSL : certif-rdsh	✓ Sélectionner Afficher
	OK Annuler

Si on effectue un changement, bien penser à Redémarrer le serveur

È <mark>©</mark> Sites È	e		9			
🗄 🦳 aspnet_clier		Explorer				
⊡[P RDWeb		Modifier les autorisations		teur	Compilation .NET) électr
	7	Ajouter une application	-			
	2	Ajouter un répertoire virtuel	¥=		Чој	
		Modifier les liaisons	amètri plicati	es on	Profil .NET	d'auto
		Gérer le site Web	2	Redén	narrer	
	49	Actualiser		Démar	rrer V	



VERIFICATION DES CERTIFICAT

Connexion HTTPS au portail RDWeb – FQDN et domaine:

Le problème était ce message sur (par exemple) l'URL https://rds-form/RDWeb



Lorsque l'on a certifié le serveur IIS, on a indiqué la machine **rds-form.form.edu** avec son **FQDN**,

donc Par conséquent il faut désormais accéder au portail <u>depuis une machine</u> <u>du domaine</u> avec l'adresse suivante :

https://rds-form.form.edu/RDWeb

Ce	rtificat	N	×
0	Général Détails Ch	ht emin d'accès de certification	
	Informa	tions sur le certificat	
	Ce certificat e	st conçu pour les rôles suivants :	
	• Garantit l'	identité d'un ordinateur distant	
	Délivré à :	rds-form.form.edu	
	Délivré par :	form-pki-CA	



Et on accède au portail sans erreurs...

Accès Bureau à distant	ice par le Web - Internet Explorer fourni par GA ds-form.form.edu/RDWeb/Pages/fr-FR/login.aspx	F - cabare
Fichier Edition Affichage	Favoris Outils ?	
🏠 🔹 🔜 👻 📼 🕶	🖓 Page 👻 Sécurité 👻 Outils 👻 🕡 🖉	
	Work Resources Connexions aux programmes RemoteApp et a	ux services Bureau à distance

L'effacement du cache du navigateur, et autre effets de bords peuvent rendre ce test un peu... "laborieux"



N.B : Sous EDGE on ne peut pas avoir d'informations sur le certificat...



Connexion HTTPS depuis une machine hors domaine:

Si on se trouve sur une machine hors domaine, la portée de notre certificat est non valable. par conséquent on aura une **Erreur de certificat**



Si on demande d'afficher le certificat on voit bien que le Certificat est valide... simplement on ne peut pas y accéder car on





RDS 2012 R2 – accès intranet - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 112 - Michel Cabaré -

EDITEUR APPLI REMOTEAPP INCONNU

Problème de Confiance dans l'éditeur des Applications :

Le problème était ce message d'erreur (sur la gauche) au lancement de l'application... remplacé par ce message d'avertissement (sur la droite)



ici Editeur: inconnu

ici Editeur: SRV-RDS

la pose d'un certificat pour notre serveur RDS amène un mieux... il reste à faire confiance en l'éditeur indiqué, à savoir **SRV-RDS.cabare-intra.net**...

N.B: il se peut qu'il faille réinstaller les **Remote App** (et les **.RDP**) qui auraient déjà été déclarées avant l'installation des certificats...)

Empreintes numériques SHA1:

Pour trouver la clé **sha1 empreinte numérique** on va dans la **console IIS.** On demande par clic droit d'**afficher** notre certificat , et dans l'onglet **Détails** on trouve notre **empreinte numérique**





RDS 2012 R2 – accès intranet - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 113 - Michel Cabaré -

GPO pour appliquer empreintes numériques:

Cela peut aussi se résoudre via une GPO, qui doit

- soit impacter les ordinateurs clients RDS (si on fait un accès authentifié par périphérique)
- soit impacter les utilisateurs du domaine ((si on fait un accès authentifié par login utilisateur).

La **Best practice** consiste à faire une **GPO ordinateur** ET une **GPO utilisateur**, le même réglage se trouvant à disposition dans les deux niveaux. **Configuration ordinateur / Stratégies / Modèles d'administration / Composants Windows**



-		Services Bureau à distance
	+	📔 Client Connexion Bureau à distance
		🧮 Gestionnaire de licences des services Bureau à 🤅
	+	🧮 Hôte de la session Bureau à distance

- SYS 32 - Cours TP - ver 1.3 -

A priori le plus efficace c'est la clé Spécifier les empreintes numériques SHA1 des certificats représentants des éditeurs .rdp approuvés

Paramètre	État
Redirection de périphérique USB RemoteFX	
🗄 Autoriser les fichiers .rdp issus d'éditeurs valides et les paramètres .rdp par défaut	Non configuré
📰 Autoriser les fichiers .rdp issus d'éditeurs inconnus	Activé
📰 Ne pas autoriser l'enregistrement des mots de passe	Non configuré
📔 Spécifier les empreintes numériques SHA1 des certificats représentant des éditeurs	Non configuré
📰 Demander des informations d'identification sur l'ordinateur client	Non configuré

cela se configure ainsi

Spécifier les empreintes numériques SHA1 des certificats représentant des éditeurs .rdp approuvés Paramètre précédent Paramètre suivant Non configuré Commentaire : Activé Commentaire : Désactivé Pris en charge sur : Au minimum Microsoft Windows Vista avec Service Pack 1 Options : Aide : Liste séparée par des virgules des empreintes numériques SHA1 de certificats approuvés : Ce paramètre de stratégie permet de spécifier une liste d'empreintes numériques de certificats SHA1 (Secure Hash Algorithm 1) qui représentent les éditeurs approuvés de fichirdp (Remote Desktop Protocol).	💭 Spécifier les em	preintes numériques SHA1	des certificats représentant des éditeurs .rdp approuvés
 Non configuré Commentaire : Activé Désactivé Pris en charge sur : Au minimum Microsoft Windows Vista avec Service Pack 1 Options : Aide : Liste séparée par des virgules des empreintes numériques SHA1 de certificats approuvés : Algorithm 1) qui représentent les éditeurs approuvés de fichilrdp (Remote Desktop Protocol). 	Paramètre précéd	npreintes numériques SHA1 lent Paramètre suivant	des certificats représentant des éditeurs .rdp approuvés
Options : Aide : Liste séparée par des virgules des empreintes numériques SHA1 de certificats approuvés : Ce paramètre de stratégie permet de spécifier une liste d'empreintes numériques de certificats SHA1 (Secure Hash Algorithm 1) qui représentent les éditeurs approuvés de fichil .rdp (Remote Desktop Protocol).	 Non configuré Activé Désactivé 	Commentaire : Pris en charge sur : Au	minimum Microsoft Windows Vista avec Service Pack 1
Liste séparée par des virgules des empreintes numériques SHA1 de certificats approuvés : Algorithm 1) qui représentent les éditeurs approuvés de fichi .rdp (Remote Desktop Protocol).	Options :		Aide :
	Liste séparée par de numériques SHA1	es virgules des empreintes de certificats approuvés :	Ce paramètre de stratégie permet de spécifier une liste d'empreintes numériques de certificats SHA1 (Secure Hash Algorithm 1) qui représentent les éditeurs approuvés de fichie .rdp (Remote Desktop Protocol).

- Michel Cabaré -



Donc la clé que l'on a récupérée sur le certificat

E Algoria incla cripi ci	oc numan anua		=	
🔄 Empreinte numérique	: 5a 80	c a3 90 ee 50 a1 cd a2 14		
Nom convivial	certif	f-rdsh	~	
5a 8c a3 90 ee	50 al cd a	a2 14 37 c2 b7 e5	f8	
cb cb 17 bb a3				
l faut rentrer ici la clé SHA	11 du / <u>des s</u>	serveurs RDP qui sor	nt autorisés	
🔊 Spécifier les empreintes nu	mériques SHA	1 des certificats représe	ntant des éditeurs	x
	incirques srin			
Spécifier les empreintes numéric	ues SHA1 des ce	rtificats représentant des édite	eurs .rdp approuvés	
Parametre precedent Paramet	re suivant			
O Non configuré Commentaire :				
				Ĥ
 Activé 				
○ Désactivé				\sim
Pris en charge	sur: Au minim	um Windows Vista avec Servic	e Dack 1	
2	Adminin	ium windows vista avec servic	CFOCK I	Ê
				\mathbf{x}
Options :		Aide :		
Liste cénarée nar des virgules des em	preintes	Ce paramètre de stratégie	permet de spécifier une liste	7~
numériques SHA1 de certificats app	prouvés :	d'empreintes numériques	de certificats SHA1 (Secure Hash	
200-50-1-4-21427-21-7-540-4-1-17	-h - 2	Algorithm 1) qui représent	tent les éditeurs approuvés de fichiers	
[] 590eeb0a1cda2143/c2b/ebt8cbcb1/l	cedi	aup (nemote Desktop Plo	tocol).	

Et la best practice fait que l'on applique ces deux GPO

⊿ i formation strat-ordi-empreinte-serveur-appli-remoteapp-rds ■ strat-util-empreinte-serveur-appli-remoteapp-rds strat-util-office-2010 ⊿ 📋 srv-vm

- ☐ strat-ordi-empreinte-serveur-appli-remoteapp-rds
- b i vm-pour-acces-rds

Evidemment cela ne fonctionne que pour des machines du domaine...



SSO ET AUTHENTIFICATION

Double authentification :

il n'y a pas (toujours ? ...) de relais entre l'authentification sur le portail WEB des **RemoteApp** et l'accès au serveur **RDS.** Du coup il peut y avoir 2 demandes d'authentification. par exemple lorsque

- on est sur une machine externe au domaine,
- loggué avec un compte local à cette machine,

la connexion au portail RDWeb demande un 1° login

🖉 Accès Bureau à distance par le Web - Windows Inte	rnet Explorer		
CO V https://srv-rds1.cabare-intra.net/RDWeb/	Pages/fr-FR/login.aspx 🗾 😵 Erreur de certificat	ð 🐓 🗙 📴 Bing	•
🙀 Favoris 🛛 🚔 🔁 Sites suggérés 🔹 🙋 Galerie de comp	osants W 🝷		
Accès Bureau à distance par le Web		🟠 • 🔝 • 🖃 🖶 • Page •	Sécurité 🔹 Outils 🔹 🕡 👻 🎽
12	Les a s		<u> </u>
			🐻 RD Web Access
Connexion par défe	aut aux services Bureau à App et aux services Bureau à distance	distance	
/			Aide
X	Domaine\Nom d'utilisateur : Mot de passe : Sécurité (<u>afficher les explications</u>)		
	 Ceci est un ordinateur privé. 		
puis lorsque l'on lance une F	RemoteApp		

	to RD Web Access
Connexion par défaut aux services Bureau à distance Connexions aux programmes RemoteApp et aux services Bureau à distance	
Programmes RemoteApp Bureau à distance	Aide Se déconnecter
Access 2013 Excel 2013 PowerPoint Publisher Word 2013 Bureau à 2013 2013 distance	
Sécurité de Windows Entrer vos informations d'identification Ces informations d'identification seront utilisées pour vous conner SRV-RDS1.cabare-intra.net.	cter à
Nom d'utilisateur Mot de passe Domaine :	
on demande une 2° authentification	Annuler

Cela fonctionne nativement pour les Clients Windows 8.1 et postérieurs



Mise en œuvre de SSO Single Sign On :

Si on à des versions OS antérieures à ces versions (Win7, Vista, XP ...), dans ce cas la il faudrait configurer les options de délégation d'information d'identification pour faire fonctionner le SSO avec ces OS Clients. Cela se Fait via une GPO ordinateur pour les client 7

Configuration ordinateur / Stratégies / Modèles d'administration / Système

GPO Ordinateur



puis dans Délégation d'informations d'identification on demande

Cache NV de disque	► Paramètre
Délégation d'informations d'identification	Autoriser la delegación d'informacións d'identificación par deraut avec l'autor
 Démarrage à chaud de Windows Dépannage et diagnostics Gestion de l'alimentation Gestion de la communication Internet Gestionnaire de serveur 	Autoriser la délégation d'informations d'dentification par del délégation Autoriser la délégation de nouvelles informations d'identification Autoriser la délégation de nouvelles informations d'identification avec l'aut Autoriser la délégation d'informations d'identification enregistrées Autoriser la délégation des informations d'identification enregistrées avec l'

Autoriser la délégation d'informations d'identification par défaut

🜉 Autoriser la délé	gation d'informations	d'identificati	on par défaut		-	
📷 Autoriser la délé	igation d'informations	d'identificatio	n par défaut	Paramètre précédent	Paramètre suivant	
🔿 Non configuré	Commentaire :					
Activé						
O Désactivé						
	Pris en charge sur :	Au minimun	n Windows Vist	а		
		ļ				
Options :			Aide :			
Ajoutez des serveurs Concaténer les v d'exploitation su	s à la liste : Affiche aleurs par défaut du sy périeures à	r stème	Si vous désac pas (par défa par défaut n'i Remarque : le d'identificatio	tivez ce paramètre de stra ut), la délégation des infor est pas autorisée. e paramètre Autoriser la de on par défaut peut prendre	tégie ou ne le configurez mations d'identification (légation d'informations : la valeur d'un ou de	

mais aussi ajouter les serveur dans Afficher...et la syntaxe est un peu spéciale...

TERMSRV/*

correspondra a tous les serveurs TSE

TERMSRV/cabare-intra.net

correspondra à tous les serveurs TSE du domaine

Ajoutez des serveurs à la liste : Affici	ner système	Si vous désactivez ce paramètre de stratégie ou ne le configurez pas (par défaut), la délégation des informations d'identification par défaut n'est pas autorisée.	
d'exploitation supérieures à	Afficher le	e contenu	- 🗆 🗙
	Ajoutez d	des serveurs à la liste :	
		Valeur	
	•	TERMSRV/*	
	*		

par précaution on peut remplir avec la même valeurs toutes les clés "*Autoriser la délégation...*" ce qui donnerait

Ξ 🗋	🗧 Système	📥 🛛 Paramè	etre	État
	🧮 Accès au stockage amovible	📰 Auto	oriser la délégation d'informations d'identification par défaut avec l'auth	Activé
	Accès au stockage étendu	📰 Auto	oriser la délégation d'informations d'identification par défaut	Activé
B		E Auto	oriser la délégation de nouvelles informations d'identification	Activé
	Appel de procedure distante	E Auto	oriser la délégation de nouvelles informations d'identification avec l'auth	Activé
	Cache NV de discure	Auto	oriser la délégation d'informations d'identification enregistrées	Activé
F		Auti	oriser la délégation des informations d'identification enregistrées avec l'	Activé
	Délégation d'informations d'identifications	ation 🔡 🔚 Refi	user la délégation d'informations d'identification par défaut	Non configuré
	Démarrage à chaud de Windows	Refi	user la délégation de nouvelles informations d'identification	Non configuré
Β	Dépannage et diagnostics	Refi	user la délégation d'informations d'identification enregistrées	Non configuré
sti	rat-ordi-rds-sso-single-sign			
É	tendue Détails Paramètres Délénation	h		
	strat-ordi-rds-sso-single-sig	n		
	Données recueillies le : 03/09/2013 17:0	08:14	afficher tout	
	Configuration ordinateur (activée)		masquer	
	Stratégies		masquer	
	Modèles d'administration		masquer	
	Définitions de stratégies (fich	iers ADMX) récupé	érées à partir de l'ordinateur local.	
	Système/Délégation d'inform	nations d'identif	ication <u>masquer</u>	
	Stratégie	Paramètre	Commentaire	
	Autoriser la délégation	Activé		
	d'informations			
	d'identification enregistrées			
	Ajoutez des serveurs	à la liste :		
	TERMSRV/*			
	Conceténer les veleurs	par défaut du	٨٥١٤٧٨	
	système d'exploitation :	supérieures à	AC076	
	Stratégie	Paramètre	Commentaire	
	Autoriser la délégation	Activé		
	d´informations			
	d'identification par défaut			
	Ajoutez des serveurs	à la liste :		
	TERMSRV/*			
	Concaténer les valeurs système d'exploitation s	par défaut du supérieures à	Activé	
	Stratégie	Paramètre	Commentaire	
	Autoriser la délégation de	Activé	Fvidemme	nt

cela ne fonctionne que pour les machines du domaine....



EASY-PRINT

Principe des Impressions windows :

Le processus d'impression Windows en charge deux types de données **RAW** et **EMF**. Les deux types les plus couramment utilisés, métafichier amélioré (**EMF**) et prêt pour l'impression (**RAW**), affectent différemment les performances de l'ordinateur client et de l'ordinateur serveur d'impression.

EMF

Le type **EMF** (Microsoft Enhanced MetaFile) est le type de données par défaut de la plupart des programmes Windows. Avec EMF, le document imprimé est modifié en format de métafichier, plus portable que des fichiers RAW et généralement imprimable sur une imprimante quelconque. Les fichiers EMF sont en général plus petits que les fichiers RAW pour un même travail d'impression.

RAW

Le type RAW est le type de données par défaut des clients autres que les programmes Windows. Le type RAW indique au spouleur qu'il ne faut absolument pas modifier le travail avant de l'imprimer. tout le processus de préparation du travail d'impression est effectué sur l'ordinateur client.



On peut distinguer 3 phases lorsque l'on imprime :

- l'application windows génère un fichier EMF via ses fonctions GDI (Graphic Display Interface). ce fichier est léger, et indépendant de l'imprimante à utiliser
- 2. le Sytème d'impression **Spooler** gère si l'imprimante est locale ou non
 - a. Si elle est locale, le Spooler gère la transformation (**Rendering**) en fichier **RAW** spécifique à l'imprimante donnée
 - b. Si elle n'est pas locale, transfert du fichier **EMF** vers le Sytème d'impression de l'imprimante distante qui effectuera la transformation en fichier **RAW** spécifique à l'imprimante donnée
- 3. Impression du fichier **RAW** par le périphérique.



Principe des Impressions RDS :

On peut distinguer 2 type d'impressions

Accès depuis le Serveur :

Imprimantes déclarées sur le serveur RDS en USB - LPT - TcpPort -ou imprimantes réseaux accessibles via un partage \\nomserv\nomprn

- le fichier d'impressions est crée sur le serveur RDS
- c'est le client qui fait le Rendering EMF/RAW
- Flux d'impression distinct du flux RDP
- N.B: paramétrage de l'imprimante depuis le Client



Accès depuis le Client :

Imprimantes re-mappées déclarées sur le poste de travail en USB - LPT - TcpPort (imprimantes réseaux accessibles via leur adresse IP)

- le fichier d'impressions est crée sur le serveur RDS
- Flux d'impression dans le flux RDP
- **N.B**: c'est le serveur RDS qui fait le Rendering EMF/RAW, Problème de charge et ... le même pilote doit exister entre Serveur RDS et Client





Principe de Fonctionnement :

Lorsque l'on imprime, on génère un fichier d'impression XPS (équivalent microsoft du format PDF...) Ce fichier ensuite est envoyé au client TS. On peut donc dire que si le client à une imprimante correctement installée en local, il doit pouvoir par ailleurs imprimer des fichier XPS (tout comme des PDF...)



Visioneuse XPS :

Depuis le gestionnaire de serveur on demande Ajouter des fonctionnalités







On confirme



Assistant Ajout de fonctionnalités	
Confirmer les sé	lections pour l'installation
Fonctionnalités Confirmation État d'avancement	Pour installer les rôles, les services de rôle ou les fonctionnalités suivants, diquez sur Installer.
Résultats	 Il est possible que ce serveur doive être redémarré à la fin de l'installation. Visionneuse XPS
Et c'est tout !	
Assistant Ajout de fonctionnalités	
Résultats de l'ins	stallation
Fonctionnalités Confirmation État d'avancement	Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : Visionneuse XP5 Visionneuse XP5

GPO associées aux clients:

Résultats

Pour les clients on demandera



Dans laquelle on active Utiliser d'abords le pilote d'imprimante Easy print



Et on peut demander de Rediriger uniquement l'imprimante par défaut





Pour les clients la visioneuse XPS doit être installée localement, C'est le cas par défaut des postes Seven



Microsoft XPS Document Writer

Imprimante Document ∆ffichad	P				
Nem du decument	рс. É+-+	Dropriótaira		Taille	Eour
Nom du document	Elai	Proprietaire	Pages	Talle	Sour
			_		
<u>•</u>					<u> </u>
					/
				V	
📇 Proprietes de Micro	soft XPS Document	Writer		×	
Général Partage Port	s Avancé Gestion	des couleurs Sécurit	té 🛛 À propos d	e	
Microsoft	XPS Document Write	er			
-202					
				_	
Impression sur les po	orts suivants. L'impres	sion se fera sur le pi	remier port		
sélectionné libre.					
Port Des	cription	Imprimante			
192.168 Por	t TCP/IP standard	HP Business Inkje	t 3000 PS, HP		
□ 192.168 Por	t TCP/IP standard	HP LaserJet 6P			
DFCrea PD	FCreator Redirecte	PDFCreator			
Microsof Loo	al Port	Microsoft Office	ocument Im.		
XPSPort: Por	t local	Microsoft XPS Do	cument Write		
SNAGIT6 Por	t local	SnagIt 6			
	notwork ra discov	LD Officaiet 6500	E710- f (róco		
🖶 Propriétés de Micro	soft XPS Document \	Writer			
Général Partage Port	Avancé Gestion	des couleurs Í Sácuri	τά Å propos d	- İ	
	s Andrice desilorn	des codiedrs Securi		e	
Toujours disponib	le				
O Disponible de	00:00	à 00:00)	*	
	, 				
Priorité : 1	÷				
Priorité : 1					
Priorité : 1 Pilote : Micros	oft XPS Document Wr	iter 💌	Nouveau pilo	te	



ANNEXE 1 – CONFIGURATIONS RDS

Configuration 1 serveur (+ licence) déploiement rapide :

Une installation de base RDS comporte au minimum les machines suivantes avec les rôles (ou services de rôle) suivants en domaine... (un Dc doit exister)

C'est un Déploiement Rapide : ventilation sur un seul serveur unique puis installation du serveur de licence sur le même serveur



N.B: il faut absolument installer un Rôle de service Broker depuis la version 2012. ne pas installer le Remote Desktop Connection Broker, c'est ne pas utiliser RDS

Configuration 2 serveurs (+ licence) déploiement standard:



C'est un Déploiement standard : ventilation sur 2 serveurs puis installation du serveur de licence ou l'on peut



Configuration 3 serveurs (+ licence) déploiement standard :



C'est un Déploiement standard: ventilation sur 3 serveurs des 3 rôles, puis installation du serveur de licence ou l'on peut



ANNEXE2 – VM ET CONF

Environnement Hyper-V

On est sur un serveur avec Hyper-V 3.0 correspondant à Windows 2012r2,

On doit disposer au minimum de 4 Disques

- D'un disque pour l'hôte hyper-V
- D'un disque pour la VM qui sera le CD du domaine
- D'un disque pour la VM qui sera le serveur RDS
- D'un disque pour la VM qui sera notre passerelle

De Ram en quantité suffisante 4+4+4+8+

- 4G pour l'hôte hyper-V
- 4G pour la VM qui sera CD ou Gateway
- 8G ou plus pour la VM qui sera le serveur RDS

Ce qui compte pour le portage des Vm d'un hyperviseur à un autre c'est le nom du commutateur virtuel ici "*lan virtuel intra*"

5	Gestion	naire de commutateur virtuel pour SRV-V2
	 Commutateurs virtuels Nouveau commutateur réseau virtuel Ian virtuel intra Contrôleur Realtek PCIE GBE Family Extensions Paramètres du réseau global Plage d'adresses MAC 0A-0A-0A-0A-0A-00 à 0A-0A-0A-0 	Propriétés du commutateur virtuel ^ Nom :

ainsi que les plages d'adresses mac (si elles sont définies)



On se créera par exemple un Domaine form.edu

Serveur DC

- dc-form
- 192.168.1.200

Serveur RDS

- Rds-form
- 192.168.1.201 (avec dns en 192.168.1.200)



Création d'une VM à partir d'un vhd existant

Pour utiliser un disque vhd avec une Vm attention aux générations de VM !

On utilisera un disque Vhd contenant par exemple une vm windows 2012r2 std correctement préparé avec sysprep

On va dans hyper-V se créer une Vm nommée **dc-form** (pour y installer le domain controller du domaine formatione.edu)

30	Assistant Nouvel ordinateur virtuel		
Spécifier le n	om et l'emplacement		
Avant de commencer Spécifier le nom et	Choisissez un nom et un emplacement pour cet ordinateur virtuel. Le nom est affiché dans le Gestionnaire Hyper-V. Nous vous recommandons d'utiliser un nom qui vous		
l'emplacement Spécifier la génération	permettra d'identifier facilement cet ordinateur virtuel, tel que le nom de la charge de travail ou du système d'exploitation invité.		
Affecter la mémoire	Nom : dc-form		
Configurer la mise en réseau	Veue pouvoz crócr up dessior ou utilizer up dessior ovistant neur stadkar l'ardinatour virtual. Si veue po		
Connecter un disque dur virtuel	sque dur sélectionnez pas de dossier du duisier un dussier existant pour stocker for unateur vir del, si vous ne sélectionnez pas de dossier, l'ordinateur virtuel est stocké dans le dossier par défaut configuré pour ce serveur.		
Options d'installation	Stocker l'ordinateur virtuel à un autre emplacement		
Résumé Emplacement : D:\ Parcou			

De **génération 1 ou 2**, utilisant **2048** mg de Ram, utilisant le **réseau virtuel**, et en précisant que <u>l'on attachera ultérieurement</u> un disque dur

Attacher un disque dur virtuel ultérieurement

Utilisez cette option pour ignorer cette étape et attacher un disque dur virtuel existant ultérieurement.

Cela crée une structure de stockage du genre



On crée manuellement un dossier **Virtual Hard Disks** dans lequel on copie notre fichier **vhd** contenant notre vm **srv-2012-R2-std-64bits-SYSPREP.vhdx** en le renommant **dc-form.vhdx**... pour obtenir quelque chose du genre



On va attacher notre disque à notre vm dans hyper-v...

Dans les paramètres de la Vm on demande d'ajouter un disque dur



N.B : si la vm est de génération 1 on ajoute un disque IDE





	Paramètres pour dc-form sur SN-51
dc-form 🔹	
Matériel Ajouter un matériel BIOS Démarrer à partir de CD	Disque dur Vous pouvez modifier la façon dont ce disque dur virtuel est attaché à l'ordinateur virtuel. Si un système d'exploitation est installé sur ce disque, la modification de l'attachement pour tempérère d'exploitation rest installé sur ce disque, la modification de
2048 Mo	Contrôleur : Emplacement :
Processeur 1 processeur virtuel	Contrôleur IDE 0 0 (en cours d'utilisation)
E Contrôleur IDE 0 Disque dur dc-form.vhdx	Vous pouvez compacter, convertir, étendre, fusionner, reconnecter ou réduire un disque dur virtuel en modifiant le fichier associé. Spécifiez le chemin d'accès complet au fichier.
Contrôleur IDE 1	Disque dur virtuel : D:\dc-form\Virtual hard Disks\dc-form.vhdx
 Contrôleur SCSI Carte réseau 	Nouveau Modifier Inspecter Parcourir

N.B : si la vm est de génération 2 on ajoute un disque SCSI

P	aramètres pour dc-form sur SN-51
dc-form 🗸	▲ ▶ Q.
Matériel Ajouter un matériel Microprogramme Démarrer à partir de Carte réseau Mémoire 2048 Mo	Contrôleur SCSI
Processeur I processeur virtuel	Lecteur de DVD
Carte réseau Nouveau commutateur virtuel Gestion	Ajouter





2 VM minimum, CD et RDS

Il serait bon de se créer 2 Vm de la sorte, sur 2 disques, une qui sera notre DC... nommée par exemple **dc-form**,



et une autre qui sera le Serveur RDS nommée par exemple rds-form



Montage du CD de domaine

Pour monter notre serveur dc dans la vm il faut vérifier - donner

- Nom machine / Adresse Ip + passerelle + dns / Mises à jour de sécurité
- Ajout du Rôle AD DS
- Configuration du CD

Ajout du rôle AD DS

Un fois donc paramétré le serveur II faut ensuite ajouter le **Rôle AD-DS** via le gestionnaire de Rôle



Demander une installation basée sur un rôle



On choisit notre serveur





http://www.cabare.net Page 129 - Michel Cabaré -

è	Assistant A	Ajout de rôles et de fo	nctionnalités 📃 🗖 🗙
Sélectionner le se	erveur de de	stination	SERVEUR DE DESTINATION dc-form
Avant de commencer Type d'installation Sélection du serveur	Sélectionnez le ser	veur ou le disque dur virtue n serveur du pool de serveu n disque dur virtuel	l sur lequel installer des rôles et des fonctionnalités. rs
Rôles de serveurs	Pool de serveurs	5	
Fonctionnalités			
Confirmation	Filtre :		
Résultats	Nom	Adresse IP	Système d'exploitation
	dc-form	192.168.1.200	Microsoft Windows Server 2012 R2 Datacenter

On demande les services AD DS

A	Assistant Ajout de ré	èles et de fonctionnalités	_ D X
Sélectionner des rô	les de serveurs	SER	VEUR DE DESTINATION dc-form
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	Sélectionnez un ou plusieurs ró Rôles Serveur DHCP Serveur DNS Serveur Web (IIS) Services AD DS Services AD FS (Active	Directory Federation Service Directory Liphowicht Directory Liphowicht D	iomaine Active i) stockent des ropos des objets sur ient ces ponibles pour les : administrateurs du ces AD DS utilisent e domaine pour
Et on accepte fonctionnalités qui s'y	toutes les rattachent	Assistant Ajout de rôles et de fo Aiouter les fonctionnalités requises p	onctionnalités
On ne demande rie ce qui est propo fonctionnalités (p l'assistant à ajouter aura besoin)	n de plus que osé dans les oar défaut ce dont on	Vous ne pouvez pas installer Services AD DS sa rôle ou les fonctionnalités suivants sont égalen [Outils] Gestion de stratégie de groupe Outils d'administration de serveur distant Outils d'administration de rôles Outils AD DS et AD LDS Module Active Directory pour V Outils AD DS [Outils] Centre d'administrat [Outils] Composants logiciel (III Inclure les outils de gestion (si applicable) Ajouter des fonction	uf si les services de nent installés. Vindows PowerShell tion Active Directory s enfichables et outils e
a	Assistant /	Ajout de rôles et de fonctionnalités	
Sélectionner Avant de commeno Type d'installation Sélection du serveu Rôles de serveurs Fonctionnalités	des fonctionnali ser Sélectionnez une o Fonctionnalités P L Fonctionn P Gestion du Gestion du	tés pu plusieurs fonctionnalités à installer sur le serveur Des alites de .NET Framework 3.0 ^ Incl alités de .NET Framework 4.5 (2 sur 7 ins e stratégie de groupe u stockage Windows basé sur des norme	SERVEUR DE DESTIN d sélectionné. cription ut l'ensemble de WoW64 o intégralité pour prendre e rge les applications 32 bits rs d'exécution sur les allations minmales Cette



RDS 2012 R2 – accès intranet - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 130 - Michel Cabaré -

On à une petite information sur Ad et les DNS

h		Assistant Ajout de rôles et de fonctionnalités	_ _ ×
S	ervices de doma	ine Active Directory	SERVEUR DE DESTINATION dc-form
	Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités	Les services de domaine Active Directory (AD DS) stockent des info ordinateurs et les périphériques sur le réseau. Les services AD DS p gérer ces informations de façon sécurisée et facilitent le partage d les utilisateurs. Ils sont aussi nécessaires pour certaines application que Microsoft Exchange Server, et pour d'autres technologies Win de groupe.	ormations sur les utilisateurs, les permettent aux administrateurs de les ressources et la collaboration entre is fonctionnant avec annuaire, telles idows Server, telles que les Stratégies
	AD DS	A noter :	

Une confirmation

	Assistant Ajout de rôles et de fonctionnalités	
Confirmer les sélect Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD DS Confirmation Résultats	Assistant Ajout de rôles et de fonctionnalités EIONS d'Installation Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectio Installer. Redémarrer automatiquement le serveur de destination, si nécessaire Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas insta fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher. Gestion de stratégie de groupe Outils d'administration de serveur distant Outils d'administration de rôles Outils AD DS et AD LDS	DE DESTINATION dc-form nné, cliquez sur affichées sur ller ces
	Outils AD DS Centre d'administration Active Directory Composants logiciels enfichables et outils en ligne de commande A Services AD DS Exporter les paramètres de configuration Spécifier un autre chemin d'accès source Précédent Suivant > Installer	D DS

Et on demande Installer



Progression de l'i	Installation dc-form
Avant de commencer	Afficher la progression de l'installation
Type d'installation	i Installation de fonctionnalité
Sélection du serveur	
Rôles de serveurs	Installation démarrée sur dc-form
Fonctionnalités	Gestion de stratégie de groupe
AD DS	Outils d'administration de serveur distant
Confirmation	Outils d'administration de rôles
Résultats	Module Active Directory pour Windows PowerShell
	Outils AD DS
	Centre d'administration Active Directory
	Composants logiciels enlichables et outils en lighe de commande AD DS
	Services AD DS
	Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche. Exporter les paramètres de configuration
	< Précédent Suivant > Fermer Annuler
btenir	

Configuration du Serveur

Dans le gestionnaire de serveur il est indiqué qu'une tâche est en attente... Promouvoir ce serveur en contrôleur de domaine. c'est le remplacement du DCpromo qui existait sous 2008R2 !



On veut créer un nouveau domaine dans une nouvelle forêt..., il faut donc demander Ajouter une nouvelle forêt

🚡 Assis	tant Configuration des services de domaine Active Directory	_ D X
Configuration de	déploiement	SERVEUR CIBLE dc-form
Configuration de déploie Options du contrôleur de Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation	Sélectionner l'opération de déploiement Ajouter un contrôleur de domaine à un domaine existant Ajouter un nouveau domaine à une forêt existante Ajouter une nouvelle forêt Spécifiez les informations de domaine pour cette opération Domaine :	Sélectionner

RDS 2012 R2 – accès intranet

– SYS 32 – Cours TP - ver 1.3 -



http://www.cabare.net Page 132 - Michel Cabaré -

Et indiquer le nom de domaine, par exemple form.edu

Sélectionner l'opération de déploiement	t	
 Ajouter un contrôleur de domaine à Ajouter un nouveau domaine à une s Ajouter une nouvelle forêt 	un domaine existant forêt existante	
Spécifiez les informations de domaine pour cette opération		
Nom de domaine racine : form.edu		

N.B: Un domaine crée à partir d'un serveur 2012 r2 est minimum à 2012r2 ! ..., on n'oublie pas d'ajouter un DNS (le catalogue Global est coché par défaut) et le mot de passe fort de restoration (par exemple Restore-2012...)

🚡 Assi	stant Configuration des services de	domaine Active Directory	_ D X
Options du contr	ôleur de domaine		SERVEUR CIBLE dc-form
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur	Sélectionner le niveau fonctionnel de la Niveau fonctionnel de la forêt : Niveau fonctionnel du domaine : Spécifier les fonctionnalités de contrôle Serveur DNS (Domain Name System Catalogue global (GC)	windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2012 R2 windows Server 2012 R2 winde domaine	
Installation Résultats	Contrôleur de domaine en lecture s Taper le mot de passe du mode de rest Mot de passe : Confirmer le mot de passe :	eule (RODC) auration des services d'annuaire (DSRM)	

Le message est normal, car on ne fait pas de délégation DNS



Le nom netbios est affiché (il doit correspondre au nom DNS sans le sufixe)



On stocke les dossiers de **AD** et le dossier miroir de publication **SysVOL** dans les chemins proposés...



barren d

Assistant Configuration des services de domaine Active Directory

_ **D** X

Chemins d'accès		SERVEUR CIBLE dc-form
Configuration de déploie Options du contrôleur de	Spécifier l'emplacement de la base c	le données AD DS, des fichiers journaux et de SYSVOL
Options DNS	Dossier de la base de données :	C:\Windows\NTDS
Options supplémentaires	Dossier des fichiers journaux :	C:\Windows\NTDS
Chemins d'accès	Dossier SYSVOL :	C:\Windows\SYSVOL

On confirme,

ه A	ssistant Configuration des services de domaine Active Directory	- 🗆 X
Examiner les op	tions see	₹VEUR CIBLE dc-form
Configuration de déploi		
Options du contrôleur d	Configurez ce serveur en tant que premier contrôleur de domaine Active Directory d'un nouvelle forêt.	ne ^
attend la validatio	n de la part de l'assistant, et on peut installer	

📥 Assis	tant Configuration des services de domaine Active Directory	_ D X
Vérification de la d	configuration requise	SERVEUR CIBLE dc-form
Toutes les vérifications de l	a configuration requise ont donné satisfaction. Cliquez sur Installer pour commeAffich	ner plus 🗙
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires	La configuration requise doit être validée avant que les services de domaine Active l installés sur cet ordinateur Réexécuter la vérification de la configuration requise	Directory soient
Chemins d'accès Examiner les options Vérification de la configur	 Voir les résultats go.microsort.com/twiink/?Linkid=104721). Il est impossible de créer une délégation pour ce serveur DNS car la zone part faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows procédez à l'intégration avec une infrastructure DNS evistante yous devez 	ente . Si vous

Et le serveur re-démarre...

Il reste quelques petits réglages à effectuer pour finaliser le domaine

- Adresse DNS propre (et non pas 127.0.0.1)
- Création dans le DNS de la zone de recherche inversée
- Ajout du pointeur correspondant au DC
- Re vérification des mises à jour
- Donner un mot de passe à l'administrateur de Domaine différent de celui qui était là pour l'administrateur local

Montage du RDS de domaine

Pour monter notre serveur RDS dans la vm rds-form il faut vérifier - donner

- Nom machine / Adresse lp + Passerelle + Dns
- Mises à jour de sécurité
- Devenir membre du domaine, compte machine / Hôte / ptr / adhésion
- Ajout du Rôle via l'assistant en déploiement rapide voir le chapitre Installation Rôle RDS



ANNEXE 3 – INSTALLATION OFFICE 2010

Message au 1° lancement d'office

Lorsqu'un utilisateur va lancer office 2010 pour la première fois, il va faire apparaître cette boite de dialogue, bien connue



Cette fenêtre appelée « Assistant d'adhésion » ou « Bienvenue dans Microsoft Office 2010 » peut nécessiter de disposer de privilèges « administrateur » pour être validée

Sauf s'il y répond par **Ne pas apporter de modification**, il aboutira à une fin de non recevoir car sur le Serveur RDS il n'a aucun droit pour modifier un fichier quelconque de configuration...

Il faut donc désactiver impérativement cet affichage dans le cas d'un installation d'office 2010 en RDS

Modèles de Stratégies office 2010

Il faut récupérer les modèles de stratégies chez microsoft

Office 2010 Administrative Template files (ADM, ADMX/ADML) and Office Customization Tool download



Get the free email ap



RDS 2012 R2 – accès intranet – SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 135 - Michel Cabaré -

AdminTemplates_32.exe	15.6 MB	
AdminTemplates_64.exe	15.9 MB	
Office2010GroupPolicyAndOCTSettings_Reference.xls	2.0 MB	

Pour nous la version 32 bits nous intéresse 🔀 AdminTemplates_32.exe

Les modèles **ADM** sont les plus passe-partout, seul celui général d'office compte pour l'instant



Ensuite il faut ajouter ce modèle à nos modèles en vigueurs dans notre AD

On se crée une nouvelle GPO et on demande sur les Modèles d'administration clic droit Ajout/Suppression de modèles...



On va chercher notre office14.adm

Et on l'ajoute

Ajout/Sup	pression de modèle	s 🗾
Modèles de stratégie actuels :		
Nom	Taille	Modifié
office14	1539KB	24/08/2011 03:15

Ce qui fait apparaître un modèle **Microsoft Office 2010** dans notre liste de réglages GPO





On va dans dans **Confidentialité**, centre de gestion de la confidentialité, et on active la... désactivation de l'assistant adhésion lors de la première execution



Bien sur après il faut appliquer cette GPO sur les utilisateurs de RDS





RDS 2012 R2 – accès intranet – SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 137 - Michel Cabaré -

Installation d'office 2010 setup / admin

lancer le fichier setup.exe du CD d'Office 2010 avec le paramètre /admin

cliquer sur le bouton « Office Customization Tool » dans l'onglet « Office Products » de votre application.

neral Details Dependent	ies Office Products				
Office product to install:	Standard				•
Config.xml settings					
Office languages:	₩ fr-fr				
	Note: By default, Office Se to force installation of spec	etup will install la cific language p	nguages matching the C icks.	IS. Select langua	iges above
Product key:	Warning: Product key is st	tored in clear tex	t. Use an MSP configu	ation file to obfus	cate the value.
Customer name:	SERIES-INFO.COM				
	1				
🔽 Display level:	Basic	•			
Display level:	Basic	•			
 Display level: Accept EULA Cache only Always suppress reb 	Basic	•			
Display level: Accept EULA Cache only Always suppress reb	Basic		E dà Cantér unit	1 0.6	
Display level: Accept EULA Cache only Always suppress reb	Basic		Edit Config.xml	Office (Customization Tool

Utilisez le bouton Office Customzation Tool pour personnaliser l'installation

Dans la section Modifier les paramètres utilisateur », développer l'arborescence Microsoft Office 2010 puis confidentialité puis centre de gestion de la confidentialité.

Outil de personna	lisation Microsoft O	ffice	0
Bienvenue Installation Emplacement d'installation et nom de l'orga Sources réseau supplémentaires Licences et interface utilisateur Supprimer les installations précédentes Ajouter des installations et exécuter des pr Paramètres de sécurité Office Modifier les propriétés d'installation Fonctionnalités Modifier les paramètres utilisateur Définir les états d'installation des composar Contenu supplémentaire Ajouter des fichiers Supprimer des fichiers Ajouter des entrées de registre Configurer des naccourcis	Modifiez un paramètre utilisateur Office sur l'ord	linateur où ce fichier de personnalisation est appliqué. Seuls les paramètres conf Paramètre Désactiver l'Assistant Adhésion lors de la première exécution Activer le Programme d'amélioration du produit Réception automatique des petites mises à jour pour améliorer la fiabilité	igurés sont appliqués. Statut Activée Non configurée Non configurée
Judiook Profil d'Outlook Ajouter des comptes Exporter les paramètres Spécifier les groupes Envol/Réception	Afficher tous les paramètres C Afficher Afficher La migration des paramètres utilis Ce paramètre de stratégie contrôle l'affichage 2010.51 vous activez ce paramètre de stratégie Office 2010.51 vous désactivez ou ne configure exécutent une application Microsoft Office 201 Microsoft Update, le Programme d'amélioration	Initiation of the service of th	ation Microsoft Office utent une application s que les utilisateurs ence d'Office, tels que

On active Désactiver l'assistant adhésion lors de la première exécution

Enregistrer le fichier .MSP dans le répertoire **UPDATES** des sources d'installation d'Office 2010. Il sera pris en compte au cours du processus d'installation.



ANNEXE 4 – GESTION CERTIFICAT

Console Certificats

Lorsque sur notre serveur on a installé notre **pki racine** de domaine, on a bien un outil **autorité de certification** qui apparaît disponible

📮 certsrv - [A	utorité de certific	ation (Local)\form-pl	ki-CA\Certificats o
Fichier Action Affichage ?			
🗢 🏟 🖄 🙆 😰			
🚋 Autorité de certification (Local)	ID de la demande	Nom du demandeur	Certificat binaire
🛛 👼 form-pki-CA	2	FORM\Administrateur	BEGIN CERT
Certificats révoqués			
Certificats délivrés			
📔 Demandes en attente			
🧮 Demandes ayant échoué			
Modèles de certificats			

Pour gérer les certificats (demandes) autrement que en passant via IIS, il est possible d'installer une mmc certificats. Sur cette même machine (qui connait donc notre **pk**i) on exécute **mmc.exe**

Ajouter ou supprimer des composants logiciels enfichables							
Vous pouvez sélectionner des composants logiciels enfichables parmi ceux disponibles sur votre ordinateur, et composants logiciels enfichables extensibles, vous pouvez spécifier quelles extensions doivent être activées.							
Composants logiciels enficha	bles disponibles :			Composants logiciels enfi. sélectionnés :			
Composant logiciel enfi	Fournisseur	^		Racine de la console			
N Analyseur de perfor	Microsoft Cor						
Autorité de certifica	Microsoft Cor	_					
Certificats	Microsoft Cor	=					
👔 Configuration du clie	Microsoft Cor						
🚡 Configuration et an	Microsoft Cor						
📹 Contrôle ActiveX	Microsoft Cor						
📫 Contrôle WMI	Microsoft Cor		Ajouter >				

On demande un compte ordinateur, et ordinateur local

Composant logiciel enfichable Certificats	
Ce composant logiciel enfichable gérera toujours les certificats pour : Mon compte d'utilisateur Un compte de service Un compte d'ordinateur	
Sélectionner un ordinateur	x
Sélectionnez l'ordinateur devant être géré par ce composant logiciel enfichable. Ce composant logiciel enfichable gérera toujours :	de

Et on valide



Ajouter ou supprimer des composants logiciels enfichables Vous pouvez sélectionner des composants logiciels enfichables parmi ceux disponibles sur votre ordinateur, et les configurer. Pour les composants logiciels enfichables extensibles, vous pouvez spécifier quelles extensions doivent être activées. Composants logiciels enfichables disponibles : Composants logiciels enfichables disponibles :						
Composant logiciel enfi	Fournisseur			Racine de la console	Modifier les extensions	
Analyseur de perfor	Microsoft Cor	-		Certificats (ordinateur local)	Mounter les extensions	
Autorité de certifica	Microsoft Cor				Supprimer	
Certificats	Microsoft Cor	≡				
Configuration du die	Microsoft Cor				Mashar	
Configuration et an	Microsoft Cor				Monter	
Contrôle ActiveX	Microsoft Cor				Descendre	
Contrôle WMI	Microsoft Cor		Ajouter >			
A DNS	Microsoft Cor					
Domaines et approb	Microsoft Cor					
Dossier	Microsoft Cor					
👸 Dossiers partagés	Microsoft Cor					
Éditeur d'objets de s	Microsoft Cor					
Éditeur d'objets de s	Microsoft Cor					
Éditeur de aestion d	Microsoft Cor	\sim			Avancé	
Description : Le composant logiciel enfichable Certificats vous permet de parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur.						
				[OK Annuler	

On peut vérifier que

Console1 - [Racine de la console\Certifica	ts (ordinateur local)\Autorités c	le certification racines de conf	iance
🚟 Fichier Action Affichage Favoris Fenêtre ?			
🗢 🄿 🙍 📋 🔍 🔂 📷			
📔 Racine de la console	Délivré à	Délivré par	Date
⊿ Gertificats (ordinateur local)	🛱 Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	02/0
Personnel	🛱 Copyright (c) 1997 Microsoft C	Copyright (c) 1997 Microsoft Corp.	31/1
Autorités de certification racines de confiance	🔄 form-pki-CA	form-pki-CA	01/0
Certificats	🔄 form-pki-CA	form-pki-CA	01/0
▷ Confiance de l'entreprise	🛱 Microsoft Authenticode(tm) Ro	Microsoft Authenticode(tm) Root	01/0

