

# RDS 2012 R2 - Web Access RDWA - Gateway RDG -

sys 32 - Cours & TP -

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

RDS 2012 accès externe Cours – Travaux pratiques

Michel Cabaré – Ver 1.3 – Mai 2016

<u>www.cabare.net</u>©

# TABLE DES MATIÈRES

PKI et Certificat	4
Besoin de certificats :	4
Types de Certificats et PKI	5
Déroulement gestion des certificats:	6
Création PKI de domaine:	6
Ajout rôle Service de certificats AD	6
Paramétrage du rôle Service de certificats AD	8
Renouvellement PKI de domaine:	12
Déploiement - Quels Certificats pour Quels Serveurs:	14
Demande de création de Certificat de Domaine – via IIS:	15
Export de certificat:	18
Application / import de Certificat:	19
Application du Certificat sur IIS pour SSL (vérification) :	20
Vérification des Certificat	22
Connexion HTTPS au portail RDWeb –FQDN et domaine:	22
Connexion HTTPS depuis une machine hors domaine:	23
Cateway PDC	04
Gateway RDS	24
Acces externe RDP sons passerelle port 5389	24
Acces externe avec passerelle mips 443	20
Installation sonyour Catoway	20 07
Costionnaire de passerelle configuration post déploiement	20
1 Paramétrage de la CPO CAP (utilisateurs)	31
2 Paramétrage de la CPO PAP (machines ressources)	30
3 Gestion de Certificat	33
	00
Test Gateway RDS	36
Paramétrage client RDP / Options déploiement	36
lest connexion depuis passerelle	39
paramètres Passerelle GPO collection	40
GPO CAO Délais deconnexion	40
collection session	41
Paramètres passerelle	41
Utilisation RDS via HTTPS	13
Ce que l'utilisateur ne peut plus faire	13
Ce que l'utilisateur peut faire	43
Certificat et domaine	44
machine hors domaine - certificat de domaine	44
machine du domaine - certificat de domaine	44
Portail Web via HTPS	46
Acces via portali web en nitps	46
Configuration Acces web des Services Bureau a Distance:	46
Ajour service acces web sur la passerelle:	4/
Ajour compte ordinateur aans groupe local KDS Enapoint:	48
Certificat public	49





http://www.cabare.net Page 2 - Michel Cabaré -

Certificat public	49
importer le certificat dans IIS:	
1 serveur = 1 certificat:	
Annexe 4 – mmc certsrv	53
Console Certificats	53



## 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)

Conne	xion Bureau à distanc	e X
🛞 U Pi	uter un programme RemoteApp. L'éditeur de ce s être identifié.	
Cette con bas, sauf	nexion distante peut endo si vous connaissez l'origir	immager votre ordinateur local ou distant. Ne vous connectez ne de cette connexion ou si vous l'avez déjà utilisée.
	Éditeur :	Serveur de publication inconnu
39	Type :	Connexion Bureau à distance
	Ordinateur distant :	SRV-RDS.cabare-intra.net
Autoriser I	l'accès de l'ordinateur dist	ant aux ressources suivantes de mon ordinateur :
	Lecteurs	Ports
	Presse-papiers	Autres périphériques PnP pris en charge
	Imprimantes	
Détai	ils	Connexion
Rem	oteāna	
- Recitin	occupp	
8	Un site Web veut programme ne per	exécuter un programme RemoteApp. L'éditeur de ce at pas être identifié
Ce prog	ramme RemoteApp p r l'exécuter sauf si vi	eut endommager votre ordinateur local ou distant. Ne vous connectez
01000		· · · · · · · · · · · · · · · · · · ·
		Convey r do subligation inconny
	Éditeur :	Serveur de publication inconno
40	Editeur : Type :	Programme RemoteApp
40	Éditeur : Type : Chemin d'accès :	Programme RemoteApp WINWORD
₩3	Editeur : Type : Chemin d'accès : Nom :	Programme RemoteApp WINWORD Word 2013



# 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
- 3. 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 Serveur RDS. C'est le rôle nommé Services de certificats Active Directory

Sélectionner des	rôles de serv	eurs	SERVEUR DE DESTINATION dc-form.form.edu
Avant de commencer Type d'installation	Sélectionnez un ou Rôles	plusieurs rôles à installer sur le serveur sé	lectionné.
Sélection du serveur Rôles de serveurs Fonctionnalités AD CS Services de rôle Confirmation Résultats	<ul> <li>✓ Serveur DN:</li> <li>Serveur Wei</li> <li>✓ Services AD</li> <li>Services AD</li> <li>Services AD</li> <li>Services AD</li> <li>Services AD</li> <li>Services AD</li> <li>Services d'a</li> <li>Services d'a</li> <li>Services de</li> </ul>	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 déploiement Windows	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 ssociées	fonctions	Assistant Ajout de rôles Ajouter les fonctionnalités re certificats Active Directory ?	et de fonctionnalités X quises pour Services de
		fonctionnalité, mais ils ne doivent pa sur le même serveur.     Outils d'administration de serve     Outils d'administration de rê Outils d'administration de cerve Outils des services de cer IOutils 1 Outils de aest	s obligatoirement être installés ur distant des tificats Active Directory ion de l'autorité de certification

- SYS 32 - Cours TP - ver 1.3 -



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

<b>a</b>	Assistant Ajout de rôles et de fonctionnalités	_ <b>_</b> 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	<ul> <li>Les paramètres de nom et de domaine de cet ordinateur ne sor</li> </ul>	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

	<b>a</b>	Assistant Ajout de rôles et de fonctionnalités	
	Sélectionner des s	ervices de rôle	SERVEUR DE DESTINATION dc-form.form.edu
	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.
On cor	nfirme		
	<b>a</b>	Assistant Ajout de rôles et de fonctionnalités	
	Confirmer les séle	ctions d'installation	SERVEUR DE DESTINATION dc-form.form.edu
	Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités	Pour installer les rôles, services de rôle ou fonctionnalités suiv Installer. Redémarrer automatiquement le serveur de destination, Il se peut que des fonctionnalités facultatives (comme des our cette page, car elles ont été sélectionnées automatiquement. fonctionnalités facultatives, cliquez sur Précédent pour désact	rants sur le serveur sélectionné, cliquez sur si nécessaire tils d'administration) soient affichées sur Si vous ne voulez pas installer ces iver 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	



http://www.cabare.net Page 7 - Michel Cabaré -

## Et cela s'installe

æ	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
	<ul> <li>Repondeur en ligne</li> <li>Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs d'entreprise :         <ul> <li>Autorité de certification d'entreprise</li> <li>Service Web Stratégie d'inscription de certificats</li> <li>Service Web Inscription de certificats</li> <li>Service Original d'entreprise</li> </ul> </li> </ul>
	Informations d'identification : FORM\Administrateur Modifier
	En savoir plus sur les rôles de serveur AD CS
	< Précédent Suivant > Configurer Annuler



**RDS 2012 R2 – accès externe** - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 8 - Michel Cabaré -

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

<b>B</b>	Configuration des services de certificats Active Directory	_ <b>_</b> ×
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 I	Configuration des services de certificats Active Directory	_ <b>D</b> X
Type d'autorité de	ecertification	SERVEUR DE DESTINATION 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 sommet de la hiérarchie PKI et émet ses propres certificats auto-sig	certification racine se trouve au nés. Une autorité de
Clé privée	certification secondaire reçoit un certificat de l'autorité de certificati	on de rang plus élevé dans la
Chiffrement	hiérarchie PKI.	
Nom de l'AC	<ul> <li>Autorité de certification racine</li> </ul>	
Période de validité	Les autorités de certification racines sont les premières voire les configurées dans une biérarchie PKI	seules autorités de certification
Base de données de certi	comigurees dans die merarchie PKI.	
Confirmation	<ul> <li>Autorité de certification secondaire</li> </ul>	
Progression	Les autorités de certification secondaires nécessitent une hiérarci autorisées à émettre des certificats par l'autorité de certification	hie PKI établie et sont de rang plus élevé dans la
Résultats	hiérarchie.	



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>b</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	Oréer une clé privée
Chiffrement	Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.
Nom de l'AC	O 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.	<ul> <li>Sélectionner un certificat et utiliser sa clé privée associée</li> </ul>

## On garde le chiffrement proposé RSA 2048 SHA1

<b>b</b>	Configuration des services de certificats Active Directory	_ <b>□</b> 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>b</b> (	Configuration des services de certificats Active Directory	_ <b>D</b> 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>a</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	es de rôle ou fonctionnalités ci-après, cliquez sur Configurer.
Services de rôle	<ul> <li>Services de certificats Acti</li> </ul>	ive Directory
Type d'AC Clé privée	Autorité de certification Type d'AC :	Racine d'entreprise
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	Nom unique :	CN=form-pki-CA,DC=form,DC=edu
Résultats	Emplacement de la base de données de certificats :	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 externe** - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 11 - 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 (¥0.0) Avertisse	cabare-pki-CA (¥0.0) Avertissement			
E P Roles	Nom	Statut	Date d'expiration		
	🗔 Certificat d'autorité de certific	ОК	23/04/2017 18:42		
🕀 🙀 Services Bureau à distance	🗐 🖈 Emplacement de AIA #1	OK	23/04/2017 18:42		
Services de certificats Active Directory	🛛 🔏 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 (SF 🗆 🖹 Pôles	RV-DC)	cabare-pki-CA	
<ul> <li>➡ ₩ Koles</li> <li>➡ ¥ Serveur DHCP</li> <li>➡ Services Bureau à d</li> <li>➡ ♀ Services de certifica</li> <li>➡ ♀ Services de certifica</li> <li>➡ ♀ PKI d'entreprise</li> <li>↓ abare-pki-CA</li> </ul>	listance ats Active Directory : CA (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 <sup>=</sup> 🛅 Demandes	Affichage 🕨 .	Arrêter le service	
Demandes Actualiser Modèles de Exporter la liste		Soumettre une nouvelle demande Sauvegarder l'autorité de certification	
<ul> <li></li></ul>	Propriétés	Restaurer l'autorité de certification Renouveler le certificat d'autorité de certification	
	Aide	κ	



http://www.cabare.net Page 12 - Michel Cabaré -

#### un message apparaît

Les services de certificats Active Directory ne pendant cette opération. Voulez-vous arrêter Active Directory maintenant ?	peuvent pas s'exécuter les services de certificats
	Renouveler le certificat d'autorité de certification
<b>NON,</b> 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: Im

et on obtient le renouvellement



# Voici quelques certificats types

Certificats délivré	źs				
ID de la demande	Nom du demandeur	Certificat binaire	Modèle de certificat	Numéro de série	Date d'effet du certificat
<b>2</b>	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
<b>5</b> 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
<b>I</b>	CABARE-INTRA\SR	BEGIN CERT	Contrôleur de domaine (DomainController)	18ed905700000	13/03/2013 00:14
<b>1 1 1 1 1 1 1 1 1 1</b>	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

<b>b</b>	Propriétés de déploiem	ent		_ □	x
Configurer le dépl	oiement				
Afficher tout Passerelle des serv + Gestionnaire de lic + Accès Web des ser + Certificats –	Gérer les certificats Un déploiement des services Bureau à l'authentification du serveur, pour l'au connexions sécurisées. Le niveau de certification actuel du dé Qu'est-ce qu'un niveau de certification	distance requiert des thentification unique ploiement est <b>Non co</b> 2	s certificats pou et pour l'établ onfiguré	ur issement de	
	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'authentif services Bureau à distance. Vous pouvez mettre à jour ce certificat certificat existant.	ication du serveur au t en créant un certifica	près du déploi at ou en sélect	ement des ionnant 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'appliquer 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		
< 1	I		>

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	I		>

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

	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.
Organisation :	formation
- Unité d'organisation :	informatique
Ville :	grenoble
Département/région :	isere
Pays/région :	FR v

RDS 2012 R2 – accès externe

- SYS 32 - Cours TP - ver 1.3 -



http://www.cabare.net Page 16 - Michel Cabaré - Ensuite il faut aller chercher notre autorité racine PKI par Sélectionner

	Créer un certificat	? X
ļ	Autorité de certification en ligne	
Indique il doit é Indique	ez l'autorité de certification de votre domaine qui signera le certificat. Un nom convivial tre facile à retenir. er une autorité de certification en ligne :	est nécessaire ;
		Sélectionner
Exempl	e : NomAutoritéCertification\NomServeur	
Nom c	onvivial :	

## 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 M	:\ lis	User: e à ,	s∖I joi	Admin ur de	istı la	rate sti	eur.CABARE- ratégie	-INTRA>gpupda	te /fo	orce		
L L	a	mise mise	'a'a	jour jour	de de	la la	stratégie stratégie	utilisateur d'ordinateur	s'est s'est	terminée t terminée	sans sans	erreur. erreur.

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

Créer un certificat	? X
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

Certificats	de serveur	
Utilisez cette fonction por accéder aux sites Web co	ur demander et gérer les certificats se nfigurés pour le protocole SSL.	ervant au serveur Web pour
Filtrer :	🝷 🐺 Atteindre 👒 🙀 Afficher f	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
	Certificats Utilisez cette fonction por accéder aux sites Web con Filtrer : Nom certif-rdsh	Certificats de serveur Utilisez cette fonction pour demander et gérer les certificats se accéder aux sites Web configurés pour le protocole SSL. Filtrer :      Atteindre      Afficher t Nom     Délivré à     rds-form.form.edu     certif-rdsh     rds-form.form.edu



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 Weł	n pour demander et gérer les certit b configurés pour le protocole SSL	ficats servant au serveur Web pour 	
Filtrer :	🗸 🐨 Atteindre 👒 🙀 At	fficher 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
🔺 🝶 form-pki-CA	informatique	rds-form.form.edu	grenoble	iseère
Certificats révoqués				
Certificats délivrés				
📋 Demandes en attente				

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...

Vilisez cette fonction po ccéder aux sites Web cc	de serveur our demander et gérer les cert onfigurés pour le protocole SS	ificats servant au serveur Web pour iL.
Filtrer :	🗸 🐺 Atteindre 🕞 🙀	Afficher 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

En le plaçant à un endroit accessible,

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



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

http://www.cabare.net Page 18 - Michel Cabaré -

ОК

hà

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		
/			
lan de sviet. Nes enslieskle			>
Iom de sujet : Non applicable (fficher les détails Ce certificat est requis pour l'authentif ervices Bureau à distance.	ii fication du serveur ai	uprès du dép	> Ploiement des
Vom de sujet : Non applicable (fficher les détails Ce certificat est requis pour l'authentif ervices Bureau à distance. 'ous pouvez mettre à jour ce certificat ertificat existant.	ii fication du serveur ai t en créant un certifi	uprès du dép cat ou en sél	> Ploiement des ectionnant un

On va chercher notre certificat précédemment exporté

Vo à c		Selectionner un certificat e	xistant		
	ous pouvez choisir d'appliquer le co distance ou bien vous pouvez sélec	ertificat qui est actuellement stocké sur le s ctionner un autre certificat qui est stocké da	erveur du service Br ans un fichier de cer	roker pour les co rtificat PKCS.	onnexions Bure
C	) Appliquer le certificat stocké sur	le serveur du service Broker pour les conne	xions Bureau à dista	ance	
	Mot de passe .				
۲	)Choisir un autre certificat				
	Chemin d'accès au certificat :				
	\\nas-1\commun\certificat\certi	f-rdsh.pfx			Parcourir.
	Mot de passe :				
		Le niveau de certification actuel du dép Qu'est-ce qu'un niveau de certification	ploiement est <b>Non</b> (	configuré	
		Service de role	Non configurá	Ltat	État
	N	Service broker pour les connexions	Non conligure		État Prêt à apr
		Service Broker pour les connexions	Non configuré		État Prêt à app
		Service Broker pour les connexions Accès Web des services Bureau à di	Non configuré Non configuré		État Prêt à app
		Service Broker pour les connexions Accès Web des services Bureau à di Passerelle des services Bureau à dist	Non configuré Non configuré Inconnu	 	État Prêt à app
		Service Broker pour les connexions Accès Web des services Bureau à di Passerelle des services Bureau à dist <	Non configuré Non configuré Inconnu	  	État Prêt à app
		Service Broker pour les connexions Accès Web des services Bureau à dis Passerelle des services Bureau à dist < Nom de sujet : Non applicable Afficher les détails	Non configuré Non configuré Inconnu		État Prêt à app
		Service Broker pour les connexions Accès Web des services Bureau à di Passerelle des services Bureau à dist <	Non configuré Non configuré Inconnu I	  uprès du déplo	État Prêt à app
		Service Broker pour les connexions Accès Web des services Bureau à di Passerelle des services Bureau à dist < Nom de sujet : Non applicable Afficher les détails Ce certificat est requis pour l'authentifi services Bureau à distance. Vous pouvez mettre à jour ce certificat	Non configuré Non configuré Inconnu ication du serveur a en créant un certifi	  uprès du déploi icat ou en sélect	État Prêt à app >



veau	Approuvé (certificat o	de domain	e) Etat <b>(</b>	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 <b>Non</b> 1 ?	configuré	É
	Le niveau de certification actuel du dé Qu'est-ce qu'un niveau de certification Service de rôle	ploiement est <b>Non</b> ? 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 <b>Non</b> ? 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 <b>Non</b> ? Niveau Approuvé Non configuré	Configuré État OK 	État Réussite
<b>,</b>	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 <b>Non</b> ? 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...

- Michel Cabaré -



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

			Liaiso	ns de sites	? 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       Toutes non attribuées         Nom de l'hôte :	Port : v 443
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				
⊡(i) RDWeb		Modifier les autorisations	ordina	teur	Compilation .NET	( électr
	7	Ajouter une application	-			
	5	Ajouter un répertoire virtuel	¥=			
		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...

e Accès Bureau à distant e e e e e e e e e e e e e e e e e e e	ce par le Web - Internet Explorer fourni par G/ ds-form <mark>.form.edu</mark> /RDWeb/Pages/fr-FR/login.aspx	NF - cabare
Fichier Edition Affichage	Favoris Outils ?	
🏠 🕶 🔜 👻 🚍 🕶	Page 🗸 Sécurité 🖌 Outils 🗸 🕢 🔊 🔊	
		24
	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** 



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 ne fait pas partie du domaine





**RDS 2012 R2 – accès externe** – SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 23 - Michel Cabaré -

Général Détails Chemin d'accès de certification

## Accès externe RDP sans passerelle port 3389

Ce mode ne fonctionne que pour donner un accès depuis l'extérieur à notre Serveur **RDS**... il rend donc accessible un serveur **RDS** à travers **HTTPS** et non plus à travers son port dédié 3386, donc sans tunnel VPN... "avant" il fallait

- 1. monter un **VPN**
- 2. chercher le serveur TSE via une @ip privée en interne (Or on ne peut pas toujours faire un **VPN**, cela peut bloquer par exemple en wifi publique, si les pare-feu n'ouvrent pas les bons ports...)

On pouvait aussi rediriger directement le port **RDP 3389** (ou autre) vers notre serveur **RDS**... mais cela posait 2 soucis

- 1. notre serveur RDS est directement exposé
- 2. le port **RDP 3389** n'est pas forcément ouvert partout... (Or on ne peut pas toujours faire transiter tous les ports cela peut bloquer par exemple en wifi publique





## Accès externe avec passerelle https 443

Avec 2012 on utilisera **https**, cela marchera tout le temps car on fait du <u>RDP</u> <u>encapsulé dans du HTTPS</u>, et le **HTTPS** est un standard en général "ouvert" partout.

l'intérêt encore une fois c'est que l'utilisateur se servira de son **client RDP** normal... ou plutôt de son navigateur standard via https.



les clients "internes" du LAN peuvent accéder aussi par la passerelle...

N.B: comme on va rediriger sur notre **Gateway RDS** tous les accès https, , cela voudra dire que si on veut d'autres services https il faudra d'autres adresses IP Publiques ! ainsi par exemple

accès RDWeb	1 @ IP publique
accès RDWeb + Webmail OWA/Exchange	2 @ ip publiques
accès RDWeb + site web en https	2 @ ip publiques
accès RDWeb + Webmail + site web en https	3 @ ip publiques

## N.B: Certificat et nom de domaine

L'utilisation d'un certificat auto signé ou même de domaine est insuffisant ici. Seul un **certificat public** donc à partir d'une **PKI publique** peut fonctionner avec une passerelle **RDS**. Si ce n'est pas possible il faudra ajouter le certificat manuellement sur la passerelle et tous les clients qui y accèdent ...

Le nom de domaine posé en intra sur la LAN doit être identique à celui du domaine déclaré pour le certificat public. Autrement dit le **nom de domaine** associé à l'adresse IP publique permettant d'arriver sur la passerelle depuis internet <u>doit être le même</u> que le **nom de domaine** LAN de l'Active Directory.



## **Redirection https et @ip gateway**

Le poste hébergeant la fonctionnalité **RDG-Gateway** devrait être une machine dédié, car dessus on installe un IIS, et l'accès Web est redirigé par définition dessus. Cela semble donc dangereux de mettre la Gateway sur un DC.

En production <u>à exclure catégoriquement</u> ! (même si c'est possible fonctionnellement pour un test ou une formation).

il faut sur le routeur rediriger les futures arrivées en https sur notre gateway

faire une règle de NAT Network Adress Translation

CONFIGURATION	NAT								
₩ Quick Setup Licensing	Configur	ration							
	No If you	ote: want to c	onfigure SNAT, p	lease go to Policy Route					
	O Ad	d 📿 Edit	Remove 🚇	Activate @ Inactivate					
+ NAT	#	Status	Name	Mapping Type	Interface	Original IP	Mapped IP	Protocol	Original Po
	1	0	rdp-poste-trava	il Virtual Server	■ wan	■ rdp-wan-poste-10	s rdp-lan-poste-10	tcp	3389
+ ALG + IP/MAC Binding	2	0	rdp-hyper-v-tra	nsf Virtual Server	<b>¤</b> wan	■ rdp-hyper-v-wan	a rdp-hyper-v-lan	any	6870
	3		gateway-rds	Virtual Server	- wan	192.168.0.2	a gateway-rds	tcp	HTTPS
	14 4	Page	1 of 1	- Shane 50 v ite	ms				
				Calt NAT					
				🔚 Create new Object 🔻					
				Conoral Sottings					
				General Settings					
				📝 Enable Rule	_				
				Rule Name:		gateway-rds			
				Port Mapping Type					
Autn. Method     Certificate				Classification:		Virtual Server	1:1 NAT	Many 1:1 NAT	
				Mapping Rule					
				Incoming Interface:		wan	*		
System				Original IP:		User Defined	*		
				Liser-Defined Or	ininal IP:	102 169 0 2 /m	Address)		
				User-Delined Or	iginar 18:	192.108.0.2	Auditess)		
				Mapped IP:		gateway-rds	~		
				Port Mapping Type:		Service	*		
				Original Service:		HTTPS	<ul> <li>TCP, 443</li> </ul>		
				Mapped Service		HTTPS	▼ TCP, 443		
				Related Settings					
								~5	

En général associée à une règle de Firewall

VPN     BWM     Ant-X     Constant     Constant	HTTPS ny
BWM     Ant-X     C Edit Firewall Rule 3     Ant-X     Ant-X     Ant-X	ny
→ User/Group	
Address     Service     Schedule     From: WAN	
AAA Server     Auth. Method     To:     LAN1     Certificate     Operation	
SSL Application     SSL Application	
Endpoint Security User: any	
Description     Description     Source: any ▼     Source:      Any ▼     Source:      S	
Destination: gateway-rds 🗸	
Service: HTTPS 🗸	
Access: allow 🗸	
Log: v	

on pourra vérifier sur des sites comme

T1 http://www.t1shopper.com/tools/port-scan/



que le nom de domaine soit bien connu des DNS

traceroute to www.cabare-intra.net (193.251.23.12), 20 hops max, 40 byte packets 1 208.64.252.229.uscolo.com (208.64.252.229) 0.329 ms 0.356 ms 0.424 ms 2 208.64.248.17.uscolo.com (208.64.248.17) 0.792 ms 0.853 ms 0.905 ms 3 69.31.114.17 (69.31.114.17) 0.693 ms 0.681 ms 0.663 ms

et que les ports soient bien ouverts et accessibles

## Scanning ports on cabare-intra.net

cabare-intra.net isn't responding on port 21 (ftp). cabare-intra.net isn't responding on port 23 (telnet). cabare-intra.net isn't responding on port 25 (smtp). cabare-intra.net is responding on port 80 (http). cabare-intra.net isn't responding on port 139 (netbios-ssn). cabare-intra.net is responding on port 443 (https). cabare-intra.net is responding on port 3389 (ms-wbt-server). cabare-intra.net isn't responding on port 5900 (). cabare-intra.net isn't responding on port 8080 (webcache).

#### **Installation serveur Gateway**



ré comme : FORM\Administrateu	r				
			Filtrer	• ≡ ۹	∎ ▼ 🔍
	→ <b>(+)</b>		Nom de domaine complet du serveur	Service de rôle insta	allé
			dc-form.form.edu	Gestionnaire de lice	nces des servio
Accès Bureau à dista	Passerelle des service	Gestionnaire de licen	RDS-FORM.FORM.EDU	Service Broker pour	les connexion
			RDS-FORM.FORM.EDU	Hôte de session Bur	eau à distance
	$\bigcirc$		RDS-FORM.FORM.EDU	Accès Web des servi	ices Bureau à c
	Service Broker pour I				

RDS 2012 R2 – accès externe

- SYS 32 - Cours TP - ver 1.3 -



http://www.cabare.net Page 27 - Michel Cabaré - on ajoute notre serveur **gtw-form** 

2	Ajo	uter Passerelle des s	ervices Bureau à (	distance	serve	eurs		x
Sélection	nner un ser	veur						
Sélection un Nom du cer	n serveur rtificat SSL	Cet Assistant vous perme déploiement. Sélectionne services Bureau à distance	t d'ajouter Passerelle z les serveurs sur lesc e.	des service quels instal	es Bur ller le i	eau à distance serveur rôle de service Passere	rs au elle des	
Résultats		Pool de serveurs			:	Sélectionné		
in a since to		Filtre :	Adresse ID	Systèm		Ordinateur FORM.EDU (1 atu form	)	
		rds-form.form.edu dc-form.form.edu gtw-form.form.edu	192.168.1.201 192.168.1.200 192.168.1.202	System	•	gtw-torm		

Un certificat auto signé est obligatoire, il doit porter le nom de la machine qui héberge les services Passerelle (et s'il s'agit, d'une ferme, le nom de la ferme), dans l'exemple gtw-from.form.edu

Ē.	Ajouter Passerelle des services Bureau à distance serveurs
Nommer le certif	îcat SSL auto-signé
Sélection un serveur Nom du certificat SSL	Les certificats SSL permettent de chiffrer les communications entre les clients des services Bureau à distance et les serveurs de passerelle Bureau à distance. Le nom du certificat SSL auto-signé doit correspondre au nom de domaine complet du serveur de passerelle Bureau à distance.
Confirmation Résultats	Nom du certificat SSL (utiliser le nom de domaine complet externe du serveur de passerelle Bureau gtw-form.form.edu
	Le nom de domaine complet doit correspondre au nom du serveur de passerelle Bureau à distance utilisé par le client des services Bureau à distance.

## On confirme en demandant Ajouter

	Ajouter Passerelle des services Bureau à distance serveurs
Confirmer les sélé	ections
Sélection un serveur	Le service de rôle Passerelle des services Bureau à distance sera installé sur les serveurs et ajouté au déploiement.
Confirmation	Passerelle des services Bureau à distance (1 serveur sélectionné)
Résultats	gtw-form.form.edu Nom complet externe de passerelle des services Bureau à distance gtw-form.form.edu

# Et c'est terminé

<b>b</b>	Ajouter Passerelle des serv	ices Bureau à distance serveurs	>
Afficher la pro	ogression		
Sélection un serveur	Le service de rôle est en cour	rs d'installation sur les serveurs suivants.	
Nom du certificat SSL	Serveur	État d'avancement	État
Confirmation	Service de rôle Passerelle	des services Bureau à distance	<b>↓</b>
Resultats	atu farm farm adu		Régeri



– SYS 32 – Cours TP - ver 1.3 -

**RDS 2012 R2 – accès externe** http://www.cabare.net Page 28 - Michel Cabaré -



Cette installation aura pour effet d'installer sur notre poste gtw-form

- Un serveur IIS,
- un Proxy RPC qui convertira le flux https/443 en RDP/3389
- un NPS Network Policy Server : qui permettra de définir des stratégies d'accès, c'est à dire permettra de spécifier qui peut "passer"... Le NPS transmettra ensuite au NAP NAP Network Acces protocol le résultat de sa décision. La Gateway RDS va donc permettre des filtrages à l'aide de NPS, il va falloir donc lister les Serveurs RDS à utiliser (on peut en effet décider de ne pas offrir sur le web tous les serveurs RDS dont on dispose...). Cela se fera sur la Gateway par la configuration de 2 GPO :
  - une GPO RDS dite CAP Connexion Access policy permettant de définir qui peut se connecter à la passerelle RDS (et cet accès est indépendant de qui peut accéder aux services des Bureaux à distance)
  - une GPO RDS dite RAP Remote Access policy permettant de définir quels sont les ordinateurs internes au LAN auxquels l'utilisateur peut avoir accès "via" la passerelle... (et ceci est indépendant de qui peut accéder à la passerelle)

**N.B** : il ne pas installer la passerelle via **Ajout de rôle**, sinon les deux stratégies précédentes ne seront pas créées par défaut.

Il reste donc fondamentalement

- A paramétrer les 2 GPO d'accès CAP et RAP
- A gérer les certificats

Déploiement configuré pour utiliser gtw-form.form.edu

Les services de rôle suivants requièrent la configuration d'un certificat : Configurer le certificat

Vérifier les propriétés de la passerelle des services Bureau à distance pour le déploiement



## Gestionnaire de passerelle configuration post déploiement

Cette console affiche de manière synthétique,

la GPO dite RAP Remote Access policy pour les serveurs RDS accessibles

| La GPO dite CAP Connexion Access policy pour les accès utilisateurs

Ainsi que le nombre de flux passant par la passerelle



Lorsque l'on se place sur un nœud, on accède aux stratégies prédéfinies,



#### soit aux propriétés du serveur passerelle



Général

Stratégies d'autorisation d'accès a

- Analyse
- Pour sécuriser les communications des écouteurs HTTPS/UDP et la messagerie NAP, un certificat est nécessaire. Le certificat est lié automatiquement aux ports HTTP et UDP configurés.

Certificat SSL

Le certificat suivant est installé sur GTW-FORM



х

Paramètres de transport

# 1 Paramétrage de la GPO CAP (utilisateurs)

Pour la 1° stratégie **CAP Connexion Access policy** permettant de définir qui peut se connecter à la **passerelle RDS** (cet accès est indépendant de qui peut accéder aux **services des Bureaux à distance**) il y a 2 points à traiter

- Qui (utilisateurs ou groupes)
- Comment on s'authentifie (mot de passe / carte à puce)

Afficher les stratégies d'autorisation des connexions
Stratégies d'autorisation des connexions
Une stratégie d'autorisation des connexions aux services Bureau à distance vo à ce serveur de passerelle Bureau à distance.
Ordre         Stratégie (appliquée selon l'ord         Groupes d'utilisateurs           Image: 1         RDG_CAP_AIIUsers         FORM\Utilisateurs du domaine

Par défaut tous les utilisateurs peuvent utiliser l'accès distant sur notre Gateway...

on va faire en sorte que seul le groupe des **Utilisateurs RDS** puissent y accéder

**N.B**: si on veut autoriser les Admins à utiliser les services de passerelle il faut ajouter le groupe Admin de domaine ici

Propriétés de RDG_CAP_AllUsers				
Général	Configuration requ	se Redirection de périphériques	Délais d'expiration	
S	RDG_CAP_AIIUse	3		
Une st vous p passer	tratégie d'autorisatio permet de spécifier relle Bureau à dista	on des connexions aux services E les utilisateurs autorisés à se con nce.	Bureau à distance necter à ce serveur de	
Nom d	le la stratégie :	RDG_CAP_utilisateurs-RDS		

On peut renommer cette GPO... pour que cela soit plus parlant

Mais surtout il faut indiquer que l'on s'authentifie par mot de passe,

Donc au final seul notre groupe d'utilisateurs à distance, plutôt que tous les utilisateurs du domaine, devrait accéder a notre passerelle avec une authentification par mot de passe

Propriétés de RDG_CAP_ut	ilisateurs-RDS	
Général Configuration requise Redirection de périp	hériques Délais d'expiration	
Spécifiez les exigences auxquelles les utilisateur connecter au serveur de passerelle Bureau à dista	s doivent se conformer pour se ance.	
Méthodes d'authentification Windows prises en ch Methodes d'authentification Windows prises en ch Methodes d'authentification Windows prises en ch	arge :	
Si vous sélectionnez les deux méthodes, l'une ou l' connexion.	autre peut être utilisée pour la	
Appartenance au groupe d'utilisateurs : (obligatoire	)	Appartenance au groupe d'utilisateurs : (obligatoire)
FORM/Utilisateurs du domaine	Ajouter un groupe	FORM\Utilisateurs-RDS
	Supprimer	
Appartenance au groupe d'ordinateurs clients : (fac	ultatif)	
	Ajouter un groupe	
	Supprimer	



# 2 Paramétrage de la GPO RAP (machines ressources)

Pour la 2° stratégie **RAP Remote Access policy** permettant de définir quels sont les ordinateurs internes au LAN auxquels l'utilisateur peut avoir accès "via" la passerelle... (Indépendamment de qui peut accéder à la passerelle) il y a 1 point à traiter

• vers quels serveurs RDS (groupe de machines accessibles)



par défaut tous les utilisateurs peuvent utiliser toutes les machines

On va faire en sorte que seul le groupe des Utilisateurs RDS puissent utiliser le groupe des serveurs RDS et on peut éventuellement la renommer

N.B : Dans notre AD il est bon de se créer un groupe global de domaine d'ordinateur correspondant aux serveurs RDS (présents, ou à venir...) par exemple serveurs-rds

ans: for	m.edu/pour-formation
itérieur à Wir	ndows 2000) :
pe	Type de groupe
	<ul> <li>Sécurité</li> </ul>
	O Distribution
	ans : for Itérieur à Wi

Serveurs RDS choisit



On peut renommer cette GPO... pour que cela soit plus parlant

Puis préciser que seuls les **utilisateurs-RDS** (et les admins de domaine si on le souhaite)

Groupe de sécurité - Global

	services b	
Général	Groupes d'utilisateurs Ressource réseau Ports autorisés	Nom de la s
Spécif aux or distan	fiez les groupes d'utilisateurs dont les membres sont autorisés à se connecter rdinateurs distants du réseau via la passerelle des services Bureau à ce.	Description
Group	es d'utilisateurs :	
FORM	/\utilisateurs-RDS	

peuvent utiliser les serveurs-RDS

	Propriétés de RDG_serveurs-RDS				
G	énéral	Groupes d'utilisateurs	Ressource réseau	Ports autorisés	
	Les utilisateurs peuvent se connecter à des ressources réseau à l'aide de la passerelle des services Bureau à distance. Les ressources réseau peuvent correspondre à des ordinateurs appartenant à un groupe de sécurité des services de domaine Active Directory ou à une batterie de serveurs Bureau à distance. Désignez la ressource réseau accessible aux utilisateurs distants en effectuant l'une des opérations suivantes :				
	Sél	lectionner un groupe de r	ressources réseau Se	rvices de domai	ne AD
	FO	RM\serveurs-rds			Parcourir



Serveurs-rds

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

# 3 Gestion de Certificat

Dans la vue d'ensemble de notre déploiement, on peut demander via les tâches de Configurer le déploiement, et visualiser l'état des certificats

# Configurer le déploiement

Afficher tout Passerelle des serv +	Gérer les certificats				
Gestionnaire de lic +					
Accès Web des ser +	Un déploiement des services Bureau à distance requiert des certificats pc l'authentification du serveur, pour l'authentification unique et pour l'étab				
Certificats –	connexions sécurisées.				
	Le niveau de certification actuel du déploiement est N Qu'est-ce qu'un niveau de certification ?	on configuré			
	Service Broker pour les connexions Approuvé	OK			
	Service Broker pour les connexions Approuvé	OK			
	Accès Web des services Bureau à di Approuvé	OK			
	Passerelle des services Bureau à dist Non configure	á <b>4</b>			

<

**N.B**: on fera faire ultérieurement une **PKI externe publique**, puis on l'importera le certificat et on l'ajoutera à notre serveur **Gateway RDS**...

111

On rejoue la même séquence que pour le certificat crée sur notre serveur **RDSH** à savoir depuis la console **gestionnaire IIS** on demande de **créer un certificat de domaine**, au nom simple de **certif-gtw** par exemple, puis on demandera de l'**Exporter** 

Connexions	Utilisez cette fonc accéder aux sites	icats de se tion pour dema Web configurés	CIVEUI ander et gérer les ce pour le protocole S	rtificats servant SSL.	: au serveur Web	pour	
Sites	Filtrer :	- 1	🔻 Atteindre 🕞 🙀	Afficher tout	Regrouper par :		
	Nom		Délivré à		Émis par		
			gtw-form.form.e	du	gtw-form.form	.edu	
	certif-gtw		gtw-form.form.e	du	form-pki-CA		
				Importer			
				Créer une de	mande de certific	:at	
				Terminer la c	lemande de certif	ficat	
				Créer un cert	ificat de domaine	e	
				Créer un cert	tificat auto-signé.		
				Afficher			
				Exporter			
				Exporter un	certificat	? X	
En le plaçant à un end	roit accessib	ole,	Exporter vers :				
			\\NAS-1\commu	un\certificat\ce	rtif-gtw.pfx		1
par exemple un empla	cement		Mot de passe :				1
\\nas-1\commun\xxxx	.pfx		•••••				
			Confirmer le mot	t de passe :			
Et 1 mot de passe iden certificats, du genre	tique pour to	ous les	•••••				]
certifxxxx				(	ОК И	Annuler	]



**RDS 2012 R2 – accès externe** - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 33 - Michel Cabaré - Pour faire propre, on fait le ménage, en supprimant le **certificat auto-signé** et en le remplaçant par le **certificat de domaine** 

Connexions 🔍 - 🔛   🖄   😥	Certific	cats de serveur	
Page de démarrage GTW-FORM (FORM\Administ	Utilisez cette fonctio accéder aux sites W	on pour demander et gérer les certifica eb configurés pour le protocole SSL.	ts servant au serveur Web pour
	Filtrer :	🕶 🖤 Atteindre 🕞 🐼 Affic	her tout Regrouper par : 👳
	Nom <sup>1</sup>	Délivré à	Émis par
	certif-gtw	gtw-form.form.edu	form-pki-CA

On va pouvoir ensuite renseigner dans notre configuration RDS que la Gateway dispose désormais d'un certificat de domaine



## On demande de sélectionner un certificat existant et

Choisir un autre certificat

Chemin d'accès au certificat :	
\\nas-1\commun\certificat\certif-gtw.pfx	
Mot de passe :	
•••••	

 Autoriser l'ajout du certificat au magasin de certificats Autorités destination

## Et on obtient

# 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 **Approuvé** Qu'est-ce qu'un niveau de certification ?

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



# Par défaut on disposait d'un certificat auto signé -

Gestionnaire de passerelle des services Bureau à distance		Propriétés de G	TW-FORM	
⊿ 🛗 Stratégies	Magasin de stratégies	s d'autorisation des conn	exions aux services Bu	reau à distance
Stratégies d'autorisation des connexions	Batterie de serveurs	Audit	Pontage SS_	Messages
🧮 Stratégies d'autorisation d'accès aux ressource	Général	Certificat SSL	Paramètr	res de transport
Analyse	Pour sécuriser les commun certificat est nécessaire. Le configurés.	ications des écouteurs H e certificat est lié automat st installé sur GTW-FOR	ITTPS/UDP et la mess iquement aux ports HT M	agerie NAP, un TP et UDP
	Délivré à : Délivré par : Date d'expiration :	gtw-form.form.edu gtw-form.form.edu 28/11/2016		
	Spécifiez le type de certific Bureau à distance en effec	at SSL à importer pour le tuant l'une des opératior	serveur de passerelle o 1s suivantes :	des services
	O Créer un certificat auto-	signé		
			Créer et importer u	n certificat
	<ul> <li>Sélectionner un certifica Certificats (Ordinateur lo</li> </ul>	at existant à partir de la p ocal)/Magasin personnel	asserelle Bureau à dista	ance GTW-FORM
	O Importer un certificat da Certificats (Ordinateur lo	ans la passerelle Bureau a ocal)/Magasin personnel	à distance GTW-FORM	1
			Paraourir ot imp	ortor un

## Maintenant on a un certificat de domaine

Gestionnaire de passerelle des services Bureau GTW-FORM (Local)	GTW-FORM (Local)		Propriétés de G	TW-FO	RM	X
Stratégies	État du serveur de p	Magasin de stratégie	s d'autorisation des conn	exions au	x services Bure	eau à distance
🦰 Analyse	État de connexion	Batterie de serveurs	Audit	Ponta	age SSL	Messages
		Général	Certificat SSL		Paramètre	es de transport
	Nombre total de co	Pour sécuriser les commur	nications des écouteurs H	ITTPS/U	DP et la messa	aerie NAP. un
	Nombre d'utilisate	certificat est nécessaire. L configurés	e certificat est lié automat	tiquement	aux ports HTT	P et UDP
	Ressources auxque	<ul> <li>Le certificat suivant e</li> </ul>	est installé sur GTW-FORI	м		
	État de configurat					
	😹 Stratégies d'auto 🐼 Stratégies d'auto	Délivré à : Délivré par :	gtw-form.form.edu form-pki-CA			
	Membres de la l distance	Date d'expiration :	01/06/2018			



٦

## Paramétrage client RDP / Options déploiement

Si on veut tester la connexion aux services via la passerelle en interne, il faut déjà dans les **Propriétés de déploiement** demander de ne pas ignorer le service de passerelle, il faut donc décocher la case **Ignorer le serveur de passerelle Bureau à distance pour les adresses locales** (coché par défaut)

Ignorer le serveur de passerelle des services Bureau à distance pour les adresses loca



Puis il faut effectuer un paramétrage du ч. Connexion Bureau à distance client RDP **Connexion Bureau** A distance Donc depuis le client RDP dans Afficher Affichage Ressources locales Programmes Expérience Avancé les Options Authentification du serveur L'authentification serveur permet de vérifier que vous vous connectez bien à l'ordinateur distant voulu. L'intensité de la vérification requise pour la connexion est déterminée par la Puis onglet Avancé / connexion depuis stratégie de sécurité de votre système tout ordinateur / Paramètres En cas d'échec de l'authentification du serveur M'avertir v Connexion depuis tout ordinateur Configurer les paramètres de connexion via la passerelle Bureau à distance lorsque je travaille à distance Paramètres. 2 Connexion Masquer les options Aide



**RDS 2012 R2 – accès externe** - SYS 32 – Cours TP - ver 1.3 - http://www.cabare.net Page 36 - Michel Cabaré -

#### il faut demander depuis le LAN

#### alors que via WAN, c'est automatique



### Puis onglet Général / Paramètres d'ouverture de session

💀 Connexion Bureau à distance 🗕 🗆 🗙						
Connexion Bureau A distance						
Général Affichage Ressources locales Programmes Expérience A · ·						
Paramètres d'ouverture de session						
	Entrez le nom de l'ordinateur distant.					
	Ordinateur : rdsform.edu 🗸					
Nom d'utilisateur :						
Vos informations d'identification seront demandées lors de la connexion.						
Me permettre d'enregistrer les informations d'identification						

**N.B:**il faut <u>indiquer ici un</u> <u>serveur RDS</u> (et non pas la Gateway, qui n'est qu'un intermédiaire) C'est pour cela que on l'a paramétrée en arrière plan!

Si on indiquait la Gateway, si tant est que l'on puisse y avoir 1 accès ouvert, on s'y arrêterait !

et donc on voit bien que l'on demande un login pour 2 connexions

Cette conne faites confia	tes-vous confiance à exion distante peut endom	n cette connexion à distance ?		
Cette conne faites confi	exion distante peut endom	nmager votre ordinateur local ou distant. Assurez-vous que vous		
	ance a I ordinateur distant	avant de vous connecter.		
	Type :	Connexion Bureau à distance		
™ Ordinateur distant : rds-form.form.edu				
	Serveur de passerelle :	gtw-form.form.edu		
Ne pasi	me redemander pour les c	connexions à cet ordinateur		
Afficher détails     Connexion Annuler				
) la pas	sserelle			

2) le serveur RDS que l'on atteindra



On peut depuis le client connecté savoir si on passe par le **port RDP 3389** ou plutôt sur le **port HTTPS 443** translaté en **NAT** pour atteindre le serveur :

**N.B**: il faut effectuer ces test <u>depuis la machine cliente</u> sur laquelle on a lancé le client RDP, et non pas dans la connexion RDP ouverte (qui se trouve donc sur le serveur RDS...)

ici on atteint le serveur RDS situé en 192.168.1.81 par le port 3389

Ca. Adı	a Administrateur : Invite de commandes				
C∶∖Us	sers\administrateur>n	etstat -an			
Conne	exions actives				
Provide the second seco	bto         Adresse locale           9         0.0.0.0:135           9         0.0.0.0:135           9         0.0.0.0:445           9         0.0.0.0:2179           9         0.0.0.0:3389           9         0.0.0.0:47001           9         0.0.0.0:49152           9         0.0.0.0:49153           9         0.0.0.0:49153           9         0.0.0.0:49154           9         0.0.0.0:49155           9         0.0.0.0:49155           9         0.0.0.0:49155           9         0.0.0.1:49155           9         0.0.0.1:49155           9         0.0.0.1:49155           9         0.2.168:1.152:13           192:168:1.152:51           192:168:1.152:51           9         192:168:1.152:51           9         192:168:1.152:51           9         192:168:1.152:51           9         192:168:1.152:51           9         192:168:1.152:51           9         1:135           10:1445           10:12:1279           10:12:13389	Adresse dista 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 9 0.0.0.0:0 9 0.0.0.0:0 9 0.0.0.0:0 9 0.0.0.0:0 544 192.168.1.61: 372 80.12.110.89: 1::1:0 1::1:0 1::1:0 1::1:0 1::1:0	nte État LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING 445 CLOSE_WAIT 445 ESTABLISHED LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING		

ici on atteint le **serveur RDS** situé en 192.168.1.81 via la **Gateway** située en 192.168.1.80 par le **port 443**, nulle par le **port 3389 n'**est utilisé ! (et encore moins une connexion sur l'adresse IP du serveur RDS 192.168.1.81...

es. Adminis	trateur : C:\Windows\system3	2\cmd.exe	
C:\Users	\Administrateur>netsta	at -a -n	
Connexio	ns actives		
Proto	Adresse locale	Adresse distante	État
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49157	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49158	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49193	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49196	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49202	0.0.0.0:0	LISTENING
TCP	127.0.0.1:2559	0.0.0.0:0	LISTENING
TCP	127.0.0.1:5354	0.0.0.0:0	LISTENING
TCP	127.0.0.1:9421	ดีดีดีดีดิเดี	LISTENING
ŤČP	127.0.0.1:9422	0.0.0.0.0	LISTENING
ŤČP	127.0.0.1:9423	0.0.0.0.0	LISTENING
ŤČP	192.168.1.10:139	0.0.0.0.0	LISTENING
ŤČP	192.168.1.10:49152	192-168-1-61:3260	ESTABLISH
TCP	192 168 1 10:49153	192-168-1-62:3260	FSTABLISH
TCP	192 168 1 10:49155	192 168 1 60:3260	FSTABLISH
TCP	192 168 1 10:49259	88 221 14 24:80	CLOSE WAT
TCP	192 168 1 10:52139	192 168 1 210:3260	FSTABLISH
TCP	192 168 1 10:53556	2 19 83 235 80	CLOSE WAI
TCP	192 168 1 10-54028	178 33 77 175-443	CLOSE HAI
TCP	192 168 1 10-54038	178 33 77 175 443	CLOSE_WHI
TCP	192 168 1 10-54048	178 33 77 175 443	CLOSE_WHI
TCP	192 168 1 10-54061	170.33.77.173.113	CLOSE_WHI
TCP	102 160 1 10 54060	170.33.77.173.113	CLOSE_WHII
TCP	102 160 1 10 54000	170.33.77.173.113	CLOSE_WHI
TCP	102.100.1.10.34070	100.JJ.((.1(J.11) 100 100 1 70.AAC	ECTADI ICUI
TCD	100 100 1 10.04100	172.100.1.72.113 190 33 99 19E.AA3	CI OCE UOI3
TCP	100 100 1 10.04100	170.33.77.173.113 170.33.77.175.113	CLOSE_WHIL
TCD	172.100.1.10.34173	170.33.77.173.443	CLOSE_WHIL
TCP	102 100 1 10-54187	170.33.77.173.443	CLOSE_WHIL
	102 100 1 10-54201	170.33.77.173.443	CLOSE_WHIL
	172.108.1.10:54215	178.33.77.175.443	CLOSE_WHI
TCP	172.108.1.10:54225		GLUSE_WHI
TCP	192.168.1.10:54263		ESTHBLISHI FOTODI IONI
TCP	192.168.1.10:54264	192.168.1.80:443	ESTRELISH
ICP	192.168.1.10:54275	178.33.77.175:443	ESTRELISH
TTP			LISTEN NO.



# Test connexion depuis passerelle

On peut du côté de la passerelle RDS vérifier si le flux passe bien par la passerelle en surveillant l'**Etat de connexion** 

🔚 Gestionnaire de serveur (SRV-GTW)	SRY-GTW (Local)
🖂 🖥 Rôles	
🕀 🐏 Serveur Web (IIS)	État du serveur de nasserelle Bureau à distance : SRV-GTW
🖃 😪 Services Bureau à distance	
🖃 😭 Gestionnaire de passerelle des services	État de connexion
🖃 🗧 SRV-GTW (Local)	
🖃 🧮 Stratégies	Nombre total de connexions 🛛 🔪 O 🔛 Surveiller les connexions actives
🧮 Stratégies d'autorisation de	Nombre d'utilisateurs connectés à ce 0
📐 🦳 Stratégies d'autorisation d'a	serveur
<sup>4</sup> ∑ 🦳 Analyse	Ressources auxquelles les utilisateurs 0
표 🎇 Configuration d'hôte de session Bureau	sont connectés
and the second second second	

# lorsqu'un utilisateur se connecte, via la passerelle on note

<ul> <li>Gestionnaire de passerelle des services Bureau</li> <li>▲ GTW-FORM (Local)</li> <li>▲ Stratégies</li> <li>▲ Stratégies d'autorisation des conn</li> </ul>	GTW-FORM (Local) État du serveur de passerelle Bureau à distance : GTW-FO	RM
Stratégies d'autorisation d'accès a Analyse	Nombre total de connexions Nombre d'utilisateurs connectés à ce serveur Ressources auxquelles les utilisateurs sont connectés	3 Surveiller les connexions actives 1 1 1
et on aura le détail via Ana	alyse ou Surveiller les connexion	s Actives

⊿	<ul> <li>GTW-FORM (Local)</li> <li>⊿ Stratégies</li> <li>≦ Stratégies d'autorisation des conn</li> <li>Stratégies d'autorisation d'accès a</li> </ul>	3 connexion(s) de 1 utilisateur(s) à 1 ordinateur(s) distant(s)				
		ID de connexion	ID d'utilisateur	Nom d'utilisateur		
	Analyse	1:1	FORM\bob	bob		
		2:1	FORM\bob	bob		
		3:1	FORM\bob	bob		



# **PARAMETRES PASSERELLE GPO COLLECTION**

# **GPO CAO Délais deconnexion**

sur notre GPO CAP on demande les propriétés

Gestionnaire de passerelle des services Bureau	Stratégi	es d'auto	orisation	des connexio	ns	
<ul> <li>▲ GTW-FORM (Local)</li> <li>▲ Stratégies</li> <li>▲ Stratégies d'autorisation des conn</li> <li>■ Stratégies d'autorisation d'accès a</li> <li>■ Analyse</li> </ul>	Une stratégie d'autorisation des connexions aux serv de passerelle Bureau à distance.					serv
	Ordre	Stratégie	e (appliqué	e selon l'ord	Gro	upe
	1	RDG_C	AP utilisat	eurs-RDS	FO	RM۱
			Dé	sactiver		
			Su	pprimer		
			Pro	opriétés		

Propriétés de RDG_CAP_utilisateurs-RDS				
Général Configuration requise Redirection de périphériques Délais d'expiration				
Spécifiez les paramètres de délai d'expiration et de reconnexion pour les sessions à distance.				
Activer le délai d'inactivité				
Déconnecter la session en cas 10 Minute(s) ndant				
Activer le délai d'expiration de la session				
Expiration de la 20 -				
Après expiration de la session :				
Déconnecter la				
Réauthentifier et réautoriser la session sans				



 A	QuickSessionCollection Propriétés	· · ·	_ □	x
Collection de sess Afficher tout	sions			
Général + Groupes d'utilisate +	Configurer les paramètres de sessi	on		
Session –	Définissez les paramètres de délai d'expiration et d session Bureau à distance pour la collection de ses	e reconnexion pour le ser sions.	rveur hôte	de
Équilibrage de la c +	Mettre fin à une session déconnectée :	Jamais		•
Paramètres du clie + Disques de profil +	Limite de la session active :	Jamais		•
	Limite de session inactive :	10 minutes		•
	Lorsqu'une limite de session est atteinte ou qu'une	connexion est interromp	ue :	
	Se déconnecter de la session			
	<ul> <li>Mettre fin à la session</li> </ul>			
	Paramètres de dossier temporaire :			
	Supprimer les dossiers temporaires en quittant			
	Utiliser des dossiers temporaires par session			

# Paramètres passerelle

sur notre passerelle on demande les propriétés

🔞 Gestionnaire de passe	relle des services Bureau GTW-FO
a 📋 GTW-FORM (Loca	
⊿ 🚞 Stratégies	Ne pas gérer ce serveur
🧮 Stratégies d	Exporter les paramètres de o
Constratégies d Stratégies d Constratégies d Stratégies	Importer les paramètres de
	Propriétés



magaain ac anaco	gies d autonsation	des connexior	ns aux service	s Bureau a	distance
Général Certificat SSL Paramètres de transport			transport		
Batterie de serveurs	Audit		Pontage SSL		Messages
Activar la massana sustàma					
Créez un message à	l'attention des utili	sateurs qui on	t ouvert une s	ession sur l	ordinateur
distant, par exemple	une notification co	ncemant la m	aintenance du	i système.	orumateur
					~
					~
					~
Heure de début :	01/06/2016	<b>]</b> ▼ 13:18:4	4		Aperçu
Heure de début :	01/06/2016	]▼ 13:18:4	4		Aperçu
Heure de début : Heure de fin :	01/06/2016	<ul><li>▼ 13:18:4</li><li>▼ 14:18:4</li></ul>	4	,	Aperçu
Heure de début : Heure de fin :	01/06/2016	]▼ 13:18:4 ]▼ 14:18:4	4		Aperçu
Heure de début : Heure de fin : Activer le message :	01/06/2016	]▼ 13:18:4 ]▼ 14:18:4	4 <u>^</u> 4 <u>^</u>		Aperçu
Heure de début : Heure de fin : Activer le message : Sélectionnez un m	01/06/2016	] ▼ 13:18:4 ] ▼ 14:18:4 sion	4 🔨	cher à l'écr	Aperçu
Heure de début : Heure de fin : Activer le message : Sélectionnez un m fois	01/06/2016	] ▼ 13:18:4 ] ▼ 14:18:4 sion ple un avis ju	4 🔨	cher à l'écr.	Aperçu
Heure de début : Heure de fin : Activer le message - Sélectionnez un m fois qu'un utilisateur ou	01/06/2016 01/06/2016 d'ouverture de ses essage, par exemp ivre une session s	] ▼ 13:18:4 ] ▼ 14:18:4 sion ple un avis ju ur l'ordinateu	4 🔨 4 🔨 ridique, à affic r distant.	cher à l'écra	Aperçu
Heure de début : Heure de fin : Activer le message Sélectionnez un m fois qu'un utilisateur ou	01/06/2016	I 3:18:4 I 14:18:4 sion ple un avis ju ur l'ordinateu	4 🔦 4 文 ridique, à affic r distant.	cher à l'écra	Aperçu



# UTILISATION RDS VIA HTTPS

# Ce que l'utilisateur ne peut plus faire

On ne peut plus se connecter directement sur le serveur RDP, on doit passer par la passerelle



les clients "internes" du LAN, eux, peuvent accéder aussi par la passerelle..., ou accéder directement au serveur RDS

## Ce que l'utilisateur peut faire

si l'utilisateur dispose sur son bureau d'un raccourcis fournis par l'administrateur permettant de lancer une application **remoteapp**, genre



2 D		

alors il peut tout simplement effectuer un double clic dessus...

WINWORD - Bloc-notes
Fichier Edition Format Affichage ?
redirectclipboard:i:1 redirectposdevices:i:0
redirectprinters:i:1 redirectcomports:i:1
devicestoredirect:s:*
redirecterives::1
prompt for credentials on client:i:1 span monitors:i:1
use multimon:i:1 remoteapplicationmode:i:1
allow font smoothing:i:1
authentication level::2
gatewaydrofileusagemethod:i:1 Joatewaycredentialssource:i:0
full address:s:SRV-RDS1.cabare-intra.net

et s'authentifier sur le portail... il aura une demande de login



Entrer vos info Ces informations suivants : 1. srv-gtw.cabar 2. SRV-RDS1.ca	ormations d'identification s d'identification serviront pour la connexion aux ordinateurs re-intra.net (serveur de passerelle Bureau à distance) bare-intra.net (ordinateur distant)	
	Nom d'utilisateur Mot de passe Domaine :	
🗌 Mémo	riser ces informations	
	OK Annuler	

# Certificat et domaine

# machine hors domaine - certificat de domaine

si on installé juste un certificat auto- signé sur notre passerelle, ou même un certificat de domaine, et que notre machine cliente ne fait pas partie du domaine,	Certificat       ×         Général       Détails       Chemin d'accès de certification         Informations sur le certificat       Windows ne dispose pas des informations suffisantes pour vérifier ce certificat.         Délivré à :       srv-gtw.cabare-intra.net         Délivré par :       cabare-pki-CA	
on ne peut se connecter depuis l'extérieur.	Valide du 09/09/2013 au 09/09/2015	
Connexion Bureau à distance		×
Cet ordinateur ne peut pas vérifier l'identité de la passerelle Bu connecter à des serveurs qui ne peuvent pas être identifiés. Co	reau à distance « srv-gtw.cabare-intra.net ». Il n'est pas prudent de se ntactez votre administrateur réseau pour obtenir de l'aide.	

# machine du domaine - certificat de domaine

 $\mathbf{k}$ 

	RemoteApp
- <b>-S</b>	Faites-vous confiance à l'éditeur de ce programme RemoteApp ?
WINWORD	Ce programme RemoteApp peut endommager votre ordinateur local ou distant. Assurez-vous que vous faites confiance à l'éditeur avant de vous connecter pour exécuter ce programme.
lancement de la	
remote app	Editeur: <u>srv-rds1.cabare-intra.net</u>
demande	Type : Programme RemoteApp
	Chemin d'accès : WINWORD
contiance de	Nom : Word 2013
l'éditeur (on non	Ordinateur distant: SRV-RDS1.cabare-intra.net
selon les GPO	Serveur de passerelle : srv-gtw.cabare-intra.net
appliquées sur le	Ne pas me redemander de connexion distante à partir de cet éditeur
client)	
,	Détails     Connexion     Annuler



ОК

Afficher le certificat...

puis evidemment authentification

			Sécurité de Windows	×
			Entrer vos informations d'identification Ces informations d'identification serviront pour la connexion aux ordinateurs suivants : 1. srv-gtw.cabare-intra.net (serveur de passerelle Bureau à distance) 2. SRV-RDS1.cabare-intra.net (ordinateur distant)	_
			Nom d'utilisateur Mot de passe Domaine :	
			OK Annuler	
	- I -	L e i	Connexion à SRV-RDS1.cabare-intra.net	en cours
remote app	ae	Ia	RemoteApp	
			Démarrage Word 2013	

warning sur certificat de domaine,

S RemoteApp	
Impossible de vérifier l'identité de l'ordinateur distant. Voulez-vous vraiment vous connecter ?	Certificat
Impossible d'authentifier l'ordinateur distant en raison de problèmes liés à son certificat de sécurité. La poursuite de l'opération peut présenter un risque. Nom du certificat Nom figurant dans le certificat de l'ordinateur distant : SRV-RDS1.cabare-intra.net	Général Détails Chemin d'accès de certification
Erreurs de certificat Les erreurs suivantes se sont produites lors de la validation du certificat de l'ordinateur distant : Ce certificat de sécurité n'émane pas d'une autorité de certification digne de confiance.	Vous ne pouvez pas faire confiance à ce certificat racine de l'autorité de certification. Pour activer la confiance, installez ce certificat dans le magasin d'autorités de certification de la racine de confiance.
Voulez-vous vous connecter malgré ces erreurs de certificat ?	Délivré à : SRV-RDS1.cabare-intra.net
Afficher le certificat Oui Non	Délivré par : SRV-RDS1.cabare-intra.net

mais on peut continuer...et lancement de la remoteapp..





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

http://www.cabare.net Page 45 - Michel Cabaré -

# **PORTAIL WEB VIA HTTPS**

# Accès Via portail web en https

On souhaite fournir sur la passerelle via **Https** un service complet de portail



## **Configuration Accès Web des Services Bureau à Distance:**

Il faut penser à indiquer dans notre vue d'ensemble, que on utilise désormais une passerelle. Dans la vue d'ensemble dans le **gestionnaire de serveur**, et demander dans les **taches** de modifier les **propriétés de déploiement** 

# Configurer le déploiement

Afficher tout Passerelle des serv –	Passerelle des services Bureau à distance
Gestionnaire de lic + Accès Web des ser + Certificats +	Paramètres de la passerelle Bureau à distance pour le déploiement O Détecter automatiquement les paramètres de serveur de passerelle des services Bureau Utiliser ces paramètres de serveur de passerelle Bureau à distance : Nom du serveur : gtw-form.form.edu Méthode d'auverture de service :
	Authentification par mot de passe       ▼         ✓       Utiliser les informations d'identification de la passerelle des services Bureau à distance pour les ordinateurs distants         □       Ignorer le serveur de passerelle des services Bureau à distance pour les adresses loca         ○       Ne pas utiliser de serveur de passerelle Bureau à distance



# Ajout service Accès Web sur la passerelle:

Si on ne veut pas obtenir un message du type

🙋 404 - Fichier ou répertoire introuvable Internet Explorer fourni par GAF - cabare	
Correction of the second secon	🔎 👻 Erreur de certificat 📄 😏 🗙 🥥 404 - Fichier ou rép
Fichier Edition Affichage Favoris Outils ?	Rěduire
🟠 🔻 🔜 🖛 👻 Page 🖌 Sécurité 🖌 Outils 👻 🕢 🐺 🔊	
Erreur de serveur	
404 - Fichier ou répertoire introuvable.	
La ressource que vous recherchez a peut-être été supprimée	ou renommée, ou est temporairement indisponible.

Et il faut pense à installer sur notre passerelle un RDWA, en effet pour l'instant sa seule machine qui héberge un rôle de portail Web c'est le serveur RDSH...

34:48   Tous les services de rôle des services TÂCH	ES 💌
● (1) ● (1)	$\odot$
Service de rôle installé	
Gestionnaire de licences des services Bureau à distanc	ce
Passerelle Bureau à distance	
Service Broker pour les connexions Bureau à distance	
Hôte de session Bureau à distance	
Accès Web des services Bureau à distance	
	34:48   Tous les services de rôle des services TÂCH

On demande donc d'ajouter un accès bureau à distance par le Web sur la machine qui héberge déjà les services de passerelle

<b>a</b>	Ajouter Accès Bureau à distance par le Web serveurs	x					
Sélectionner un serveur							
Sélection un serveur Confirmation	Cet Assistant vous permet d'ajouter Accès Bureau à distance par le Web serveurs au déploiemen Sélectionnez les serveurs sur lesquels installer le rôle de service Accès Bureau à distance par le Web.	t					
Résultats	Pool de serveurs     Sélectionné       Filtre :						
Ŀ,	srv-dc1.cabare-intra.net 192.168.1.91 SRV-GTW.cabare-intra.net 192.168.1.80						

## Et on confirme

<b>B</b>	Ajouter Accès Bureau à distance par le Web serveurs					
Confirmer les sélections						
Commenter les ser	Commentes selections					
Sélection un serveur	Sélection un serveur Le service de rôle Accès Bureau à distance par le Web sera installé sur les serveurs et ajouté au					
Confirmation	firmation					
Résultats	Résultats Accès Bureau à distance par le Web (1 serveur sélectionné)					
	SRV-GTW.cabare-intra.net					



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

http://www.cabare.net Page 47 - Michel Cabaré -

## Pour obtenir

Eiltror	0				9
ruuer	~				۲
Nom de domaine complet du serveur	Service	de rôle i	nstallé		
srv-dc1.cabare-intra.net	Gestion	naire de	licences des ser	vices Bureau à c	listance
	000000	nune ue	neenees des ser	nees baread a c	
GRV-GTW.cabare-intra.net	Passerel	lle Burea	u à distance		
SRV-GTW.cabare-intra.net SRV-GTW.cabare-intra.net	Passerel Accès W	lle Burea /eb des	u à distance services Bureau	à distance	•
SRV-GTW.cabare-intra.net SRV-GTW.cabare-intra.net SRV-RDS1.CABARE-INTRA.NET	Passerel Accès W Service	lle Burea /eb des : Broker p	u à distance services Bureau our les connexio	à distance ons Bureau à dis	
SRV-GTW.cabare-intra.net SRV-GTW.cabare-intra.net SRV-RDS1.CABARE-INTRA.NET SRV-RDS1.CABARE-INTRA.NET	Passerel Accès W Service Hôte de	lle Burea /eb des : Broker p : session	u à distance services Bureau our les connexio Bureau à distan	à distance ons Bureau à dis ice	tance

# Ajout compte ordinateur dans groupe local RDS Endpoint:

Si on ne veut pas obtenir un message du type

N.B: il faut penser à ajouter le compte ordinateur de la passerelle gtw-form dans le groupe des Serveurs RDS Endpoint sur notre serveur RDS

Pr	opriétés de : Serveurs RDS Endpoint	?	x		
Général					
Serveurs RDS Endpoint					
Description :	Description : Les serveurs de ce groupe exécutent des ordinateurs virtuels et hébergent des sessions où les utilisateurs, les programmes				
Membres :					
& AUTORITE NT\SERVICE RÉSEAU (S-1-5-20) I FORM\GTW-FORM FORM\RDS-FORM					
Pro	opriétés de : Serveurs RDS Endpoint	?	x		
Général					
Serveurs RDS Endpoint					
Description : Les serveurs de ce groupe exécutent des ordinateurs virtuels et hébergent des sessions où les utilisateurs, les programmes					
Membres :					
Image: Second Secon					



## **Certificat public**

imaginons avoir ne main un certificat public pour notre domaine, crée par exemple auprès de **startssl..** 

The Toolbox				
🔞 Help Items	PKCS#12 (PFX) Generation Successful			
<ul> <li>Theip Telms</li> <li>StartSSL<sup>TM</sup> Messages</li> <li>Add Credit Card   PayPal   Ticket</li> <li>About Smart Cards/eToken</li> <li>Submit Verification Code</li> <li>StartCom CA Certificates</li> <li>Decrypt Private Key</li> <li>Key Bug Checker</li> <li>Retrieve Certificate</li> </ul>	<ul> <li>Click in the button below to retrieve your generated PKCS#12 (PFX) file.</li> <li>Make sure you disable any download blockers and/or whitelist the startssl.com web site.</li> </ul>			

Voila notre certificat dans un fichier au format PFX

Nom 👻	Modifié le	Туре	Taille
🏂 ZcV6uP0uBrKT0PME.p12	12/09/2013 07:25	Échange d'informations personnelles	7 Ko

#### importer le certificat dans IIS:

il faut se mettre sur le **gestionnaire des services internet**, et demander d'importer le certificat.

dans notre exemple, le certificat de domaine apparaît... clic droit / Importer...

📬 Gestionnaire des services Internet (IIS)			
SRV-GTW ►			
Fichier Affichage Aide			
Connexions         Image: Connexions	Utilisez cette fonction pour accéder aux site:	<b>its de serveur</b> pour demander et gérer les certificats s Web configurés pour le protocole SSI	servant au serveur Web 
	Nom 🔺	Délivré à	Délivré par
	icertif-gtw	srv-gtw.cabare-intra.net Importer Créer une demande de certifica Terminer la demande de certific Créer un certificat de domaine. Créer un certificat auto-signé	cabare-pki-CA
et il suffit de ramener le certificat	t		

Importer un certificat ? × 13 Fichier de certificat (.pfx) : ſ ... ? X Importer un certificat Mot de passe : Fichier de certificat (.pfx) : J-dvd-sys-32-rds\start-ssl\ZcV6uP0uBrKT0PME.pfx .... 🔽 Autoriser l'exportation du certificat Mot de passe : ..... OK. Annuler 🔽 Autoriser l'exportation du certificat

## pour obtenir





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

Nom 🔺	Délivré à	Délivré par	Date d'expiration
certif-gtw	.xv-gtw.cabare-intra.net	cabare-pki-CA	09/09/2015 11:55:0
StartCom PFX Certificate	srv-gtw.cabare-intra.net	StartCom Class 1 Primary Interm	12/09/2014 21:14:1

il ne reste plus qu'à supprimer le certificat de domaine pour ne garder que le certificat public...

# Certificats de serveur

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

Nom 🔺	Délivré à	Délivré par
StartCom PFX Certificate	srv-gtw.cabare-intra.net	StartCom Class 1 Primary Interm

ensuite il faut simplement appliquer le certificat sur le site web..

## via modifier les liaisons



## importer le certificat dans gestionnaire de passerelle:

RDS 2012 R2 – accès externe

- SYS 32 - Cours TP - ver 1.3 -

Mais il faut aussi l'importer le certificat depuis notre interface gestionnaire de passerelle

6	Gestionnaire de passerelle des services Bureau à distance	_ <b>D</b> X
Fichier Action Affichage	?	
<ul> <li>Gestionnaire de passerelle</li> <li>▲ BRV-GTW (Local)</li> <li>▶ SRV-GTW (Local)</li> <li>▶ Stratégies</li> <li>▲ Analyse</li> </ul>	SRV-GTW (Local)	Actions SRV-GTW (Local)  Ne pas gérer ce serveur Exporter les paramètres de c Imonder les paramètres de
	État de configuration         Tâches de configuration           S Aucun certificat de serveur n'est installé ou sélectionné Afficher ou modifier les propriétés des certificats         Image: Configuration	Propriétés Affichage



http://www.cabare.net Page 50 - Michel Cabaré -

## On obtient



## On demande importer un certificat

Importer un certificat								
Aucun certificat n'est a	Aucun certificat n'est actuellement installé.							
Pour afficher ou installer un certificat, sélectionnez celui désiré, puis cliquez sur Afficher le certificat. Pour l'importer dans le serveur de passerelle Bureau à distance, sélectionnez le certificat, puis cliquez sur Importer.								
Délivré à	Délivré par	Rôle prévu	Date d'expirati	Remarque				
srv-gtw.cabare-i	StartCom Class 1 D	Authentification du	12/06/2017	Certificat valide				
Afficher le certificat								
Afficher tous les cettificats dans (Ordinateur local)/Magasin personnel								

**N.B**: le certificat public préalablement importé via IIS doit apparaître.

## 1 serveur = 1 certificat:

**N.B**: il faut avoir un certificat par serveur, autrement dit dans notre configuration, il faut au minimum 1 certificat pour notre passerelle **srv-gtw** et 1 certificat pour notre serveur RDS **srv-rds1**.

Si on passe en mode brooker haute disponibilité et que l'on ajoute un 2° serveur RDS il faudra bien sûr un certificat pour ce 2° serveur **srv-rds2**...

N.B: en plus de ce que l'on a fait sur notre gateway (à savoir importer le certificat, et l'appliquer au site web)

pour le (les ?) serveurs RDS il faut non seulement importer le certificat, l'appliquer au site web mais en plus appliquer le certificat au niveau RDP



😼 srv-rds1.cabare-intra.net - C	onnexion Bureau à distance		
🛞 Configuration d'hôte de sessio	on Bureau à distance		
Fichier Action Affichage ?	2		
🗇 🄿 🔲 🚺 🔽			
🥁 Configuration d'hôte de sessi ▷ ়৹∄ Diagnostic des licences	Configuration du serveur hôte d SRV-RDS1 Vous pouvez utiliser l'outil de configuration d'hôte de s connexions, modifier ceux des connexions existantes connexion par connexion, ou pour le serveur hôte de	e session Bureau à distance : Propriétés de RDP-Tcp Contrôle à distance Paramètres du client Carte réseau Sécurité Général Paramètres d'ouverture de session Sessions Environnement	
	Connexions		
	Nom de la connexion Type de connexion Ti	Type: HDP-Icp	
	■ RDP-Tcp       Microsoft RDP 6.1       tc         Modifier les paramètres       Général       []         Supprimer les dossiers temporaires en quittant	Transport : tcp Commentaire : Sécurité Couche de Sécurité : Négocier La couche la plus sécurisée prise en charge par le client sera utilisée. Si le protocole SSL (TLS 1.0) est pris en charge, il sera utilisé. Niveau de chiffrement : Compatible client	
	<ul> <li>Output des dossiers temporaires par session</li> <li>Restreindre chaque utilisateur à une seule ses</li> <li>Mode d'ouverture de session de l'utilisateur</li> <li>Gestionnaire de licences</li> <li>Mode de licence des services Bureau à dista</li> <li>Serveurs de licences des services Bureau à d</li> <li>Service Broker pour les connexions Bureau à d</li> <li>Membre d'une batterie dans le service Broker</li> </ul>	Toutes les données envoyées entre le client et le serveur sont protégées     par un chiffrement basé sur la puissance maximale prise en charge par le     client.     Autoriser les connexions uniquement à partir des ordinateurs     exécutant le Bureau à distance avec une authentification au niveau     du réseau     Certificat : <u>srv-rds1.cabare-intra net</u> Sélectionner     Par défaut     En savoir plus ur la configuration des paramètres de sécurité	

J'irais bien chercher par la sous 2012 mais je ne vois pas ou indiquer le certificat à utiliser

è	QuickSessionCollection Propriétés
Collection de sess Afficher tout Général + Groupes d'utilisate + Session + Sécurité - Équilibrage de la c + Paramètres du clie + Disques de profil +	QuickSessionCollection Propriétés         Sions         Configurer les paramètres de sécurité         Spécifiez les paramètres de sécurité entre le client et les serveurs hôtes de session Bureau à distance dans la collection de sessions.         Couche de sécurité :         Négocier         La couche la plus sécurisée prise en charge par le client sera utilisée. Si le protocole SSL (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 chiffrement basé sur la puissance de clé maximale prise en charge par le client.
	<ul> <li>Autoriser les connexions uniquement pour les ordinateurs exécutant les services Bureau à distance avec authentification au niveau du réseau</li> </ul>



# **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 certifica	ation (Local)\form-pl	ki-CA\Certificats c
Fichier Action Affichage ?			
🗢 🄿 🖄 🙆 👔			
🙀 Autorité de certification (Local)	ID de la demande	Nom du demandeur	Certificat binaire
🛛 🝶 form-pki-CA	<b>E</b>	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 pki) 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 enficitables disponibles :	_	Composants logiciels entit, selectionnes :				
Composant logiciel enfi   Fournisseur	^	Racine de la console				
🔊 Analyseur de perfor Microsoft Cor						
autorité de certifica Microsoft Cor						
Certificats Microsoft Cor						
E 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 compo O Mon co O Un cor O Un cor	osant logiciel enfichable gérera toujours les certificats pour : compte d'utilisateur ompte de service ompte d'ordinateur	
	Sélectionner un ordinateur	x
	Sélectionnez l'ordinateur devant être géré par ce composant logiciel enfichable. Ce composant logiciel enfichable gérera toujours :	

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 :						
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 ?			
<table-cell-rows> 🔿 🙍 📋 🔍 🔂 📷</table-cell-rows>			
📔 Racine de la console	Délivré à	Délivré par	Date
⊿	🔄 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

