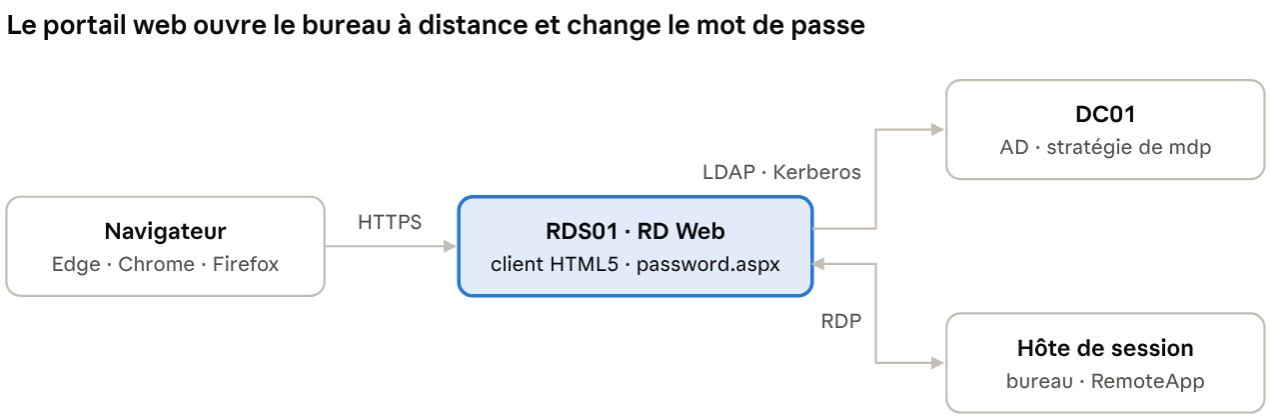
Guide d'installation — Bureau à distance web et changement de mot de passe sous Windows Server 2025

Nov 27, 2026 · @Serge Martins

Ce guide installe un portail de bureau à distance web (RD Web Access et client web HTML5) sur le serveur **RDS01** du domaine martinscie.lan, puis active le changement de mot de passe par le web. Il traite aussi le piège principal de ce service : la stratégie de mot de passe du domaine, qui bloque souvent le changement sans message clair.



RDS01 · portail web, client HTML5 et changement de mot de passe

Le navigateur ne parle qu'à RDS01 en HTTPS ; RDS01 vérifie le compte et applique la stratégie de mot de passe sur DC01, puis ouvre la session RDP.

1. Architecture et prérequis

Élément	Valeur
Serveur RDS	RDS01 · 192.168.10.51 · Windows Server 2025 Standard, membre du domaine
Rôles installés sur RDS01	RD Connection Broker, RD Web Access, RD Session Host, RD Licensing
Contrôleur de domaine	DC01 · 192.168.10.10 (AD DS, DNS, stratégie de mot de passe)
Nom d'accès	rds01.martinscie.lan (enregistrement A sur DC01)
Groupe d'accès	GG_Utilisateurs_RDS (groupe global AD)

Élément	Valeur
Clients	Postes du VLAN 20 (192.168.20.0/24), navigateur Edge, Chrome ou Firefox

Prérequis :

- RDS01 joint au domaine, IP fixe, DNS pointant sur DC01, mises à jour de novembre 2026 installées (KB5131080 pour Windows Server 2025).
- Un compte administrateur du domaine pour l'installation.
- Un certificat pour rds01.martinscie.lan : idéalement émis par une autorité de certification d'entreprise ; à défaut, un certificat auto-signé pour le lab.
- pfSense (RFW01) : autoriser le VLAN 20 vers RDS01 en TCP 443 (portail) et TCP 3389 (sessions RDP).

2. Installer le déploiement Bureau à distance

Sur RDS01, dans une console PowerShell en administrateur :

```
# Déploiement « session » complet sur un seul serveur (lab)
New-RDSessionDeployment -ConnectionBroker rds01.martinscie.lan `
  -WebAccessServer rds01.martinscie.lan -SessionHost rds01.martinscie.lan

# Serveur de licences en mode « par utilisateur »
Add-RDServer -Server rds01.martinscie.lan -Role RDS-LICENSING `
  -ConnectionBroker rds01.martinscie.lan
Set-RDLicenseConfiguration -LicenseServer rds01.martinscie.lan -Mode PerUser
`
  -ConnectionBroker rds01.martinscie.lan -Force

# Collection de sessions réservée au groupe AD
New-RDSessionCollection -CollectionName "Bureau" -SessionHost
rds01.martinscie.lan `
  -CollectionDescription "Bureau à distance Martins & Cie" -ConnectionBroker
rds01.martinscie.lan
Set-RDSessionCollectionConfiguration -CollectionName "Bureau" `
  -UserGroup "MARTINSCIE\GG_Utilisateurs_RDS" -ConnectionBroker
rds01.martinscie.lan
```

Le serveur redémarre pendant l'installation ; relancer la console ensuite. Activer le serveur de licences avec l'outil « Gestionnaire de licences des services Bureau à distance » (période de grâce de 120 jours en lab).

Option : publier une application (RemoteApp) au lieu du bureau complet :

```
New-RDRemoteApp -CollectionName "Bureau" -DisplayName "Bloc-notes" `
  -FilePath "C:\Windows\System32\notepad.exe" -ConnectionBroker
rds01.martinscie.lan
```

3. Installer les certificats

Le même certificat (format .pfx) sert au portail web, à la publication et à l'authentification unique :

```
$pwd = Read-Host -AsSecureString "Mot de passe du PFX"
foreach ($role in "RDWebAccess","RDPublishing","RDRedirector") {
  Set-RDCertificate -Role $role -ImportPath "C:\certs\rds01.pfx" -Password
$pwd `
    -ConnectionBroker rds01.martinscie.lan -Force
}
```

Pour le lab uniquement, un certificat auto-signé suffit : `New-SelfSignedCertificate -DnsName rds01.martinscie.lan -CertStoreLocation Cert:\LocalMachine\My`, puis export en .pfx (clé privée) et en .cer (clé publique). Le .cer doit être déployé dans les autorités racines de confiance des postes (GPO), sinon le navigateur affiche un avertissement.

4. Ajouter le client web HTML5

Le client web lance les sessions directement dans le navigateur, sans client RDP installé :

```
Install-Module -Name PowerShellGet -Force   # puis rouvrir la console
Install-Module -Name RDWebClientManagement
Install-RDWebClientPackage
Import-RDWebClientBrokerCert C:\certs\rds01.cer
Publish-RDWebClientPackage -Type Production -Latest
```

Adresses à retenir :

- Portail classique : `https://rds01.martinscie.lan/RDWeb`
- Client web HTML5 : `https://rds01.martinscie.lan/RDWeb/webclient`

5. Activer le changement de mot de passe par le web

La page de changement de mot de passe existe dans RD Web Access mais elle est désactivée par défaut. Elle permet aussi à un utilisateur dont le mot de passe a expiré de le renouveler.

Méthode graphique : Gestionnaire IIS → Sites → Default Web Site → RDWeb → Pages → Paramètres de l'application → `PasswordChangeEnabled` = `true`.

Méthode PowerShell :

```
Import-Module WebAdministration
Set-WebConfigurationProperty -PSPath 'IIS:\Sites\Default Web
Site\RDWeb\Pages' `
  -Filter "appSettings/add[@key='PasswordChangeEnabled']" -Name value -Value
'true'
iisreset
```

Le paramètre est enregistré dans `C:\Windows\Web\RDWeb\Pages\Web.config`. La page est ensuite accessible à l'adresse `https://rds01.martinscie.lan/RDWeb/Pages/fr-FR/password.aspx`.

Afficher un lien sur la page de connexion : l'activation n'ajoute aucun lien. Copier d'abord `C:\Windows\Web\RDWeb\Pages\fr-FR\login.aspx` (sauvegarde), puis ajouter sous le bouton de connexion une ligne du type :

```
<p><a href="password.aspx">Changer mon mot de passe</a></p>
```

Une mise à jour cumulative peut remplacer login.aspx : revérifier le lien après chaque Patch Tuesday.

6. Régler la stratégie de mot de passe (le piège)

Le changement par le web applique exactement les mêmes règles que Ctrl+Alt+Suppr. Si le nouveau mot de passe ne respecte pas une règle, Windows Server 2025 renvoie souvent un message générique (« Impossible de modifier le mot de passe pour l'instant ») sans dire laquelle. Les utilisateurs pensent alors que la page est en panne.

Où se trouve la stratégie : GPO « Default Domain Policy » → Configuration ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurité → Stratégies de comptes → Stratégie de mot de passe.

> Point clé : pour les comptes du domaine, la stratégie de mot de passe n'est lue que dans une GPO liée **à la racine du domaine**. Une GPO liée à une OU (par exemple l'OU des utilisateurs RDS) n'a aucun effet sur leurs mots de passe. Pour des règles différentes par groupe, il faut une stratégie affinée (PSO).

Paramètre	Valeur conseillée pour le lab	Effet sur le changement par le web
Longueur minimale	12 caractères	Mot de passe trop court → refus
Complexité	Activée	Pas 3 catégories sur 4, ou nom du compte inclus → refus
Historique	24 mots de passe	Réutilisation d'un ancien mot de passe → refus
Âge maximal	90 jours (ou selon la politique de l'entreprise)	Déclenche l'expiration et la page de renouvellement
Âge minimal	1 jour (base de sécurité), 0 en lab si besoin	Changement refusé si le mot de passe a moins de 1 jour
Verrouillage	5 essais, 15 minutes	Trop d'essais sur le portail → compte verrouillé

Le problème de l'âge minimal : si le dernier mot de passe a été défini il y a moins de N jours, tout changement est refusé. Cas typique : l'administrateur réinitialise le mot de passe sans cocher « L'utilisateur doit changer le mot de passe à la prochaine ouverture de session », puis l'utilisateur essaie de le changer le jour même. Avec un âge minimal de 7 ou 10 jours, le blocage dure plus d'une semaine. Solutions : garder 1 jour au maximum, toujours cocher « doit changer à la prochaine ouverture de session » lors d'une réinitialisation, ou mettre 0 jour pour un groupe via une PSO.

Stratégie affinée (PSO) pour les utilisateurs RDS :

```
New-ADFineGrainedPasswordPolicy -Name "PSO-Utilisateurs-RDS" -Precedence 10 `
  -MinPasswordLength 12 -ComplexityEnabled $true -PasswordHistoryCount 24 `
  -MinPasswordAge "1.00:00:00" -MaxPasswordAge "90.00:00:00" `
  -LockoutThreshold 5 -LockoutDuration "0.00:15:00" `
  -LockoutObservationWindow "0.00:15:00" -ReversibleEncryptionEnabled $false
Add-ADFineGrainedPasswordPolicySubject "PSO-Utilisateurs-RDS" -Subjects
"GG_Utilisateurs_RDS"
```

Vérifier ce qui s'applique vraiment :

```
Get-ADDefaultDomainPasswordPolicy                  # stratégie du domaine
Get-ADUserResultantPasswordPolicy -Identity jdupont # PSO appliquée (vide =
stratégie du domaine)
Get-ADUser jdupont -Properties
PasswordLastSet,PasswordExpired,CannotChangePassword,LockedOut
net accounts /domain
```

Vérifier aussi sur le compte que « L'utilisateur ne peut pas changer de mot de passe » n'est pas coché.

7. Tests

1. Depuis un poste du VLAN 20, ouvrir `https://rds01.martinscie.lan/RDWeb`, se connecter avec un compte de GG_Utilisateurs_RDS et lancer le bureau.
2. Ouvrir le client web (`/RDWeb/webclient`) et lancer la même ressource dans le navigateur.
3. Cliquer sur « Changer mon mot de passe », saisir un mot de passe conforme : le changement doit réussir.
4. Refaire avec un mot de passe trop court : noter le message obtenu (c'est l'occasion d'expliquer le message générique aux utilisateurs).
5. Dans l'AD, cocher « doit changer le mot de passe à la prochaine ouverture de session » sur un compte de test, puis se connecter au portail : la page de renouvellement doit s'afficher.
6. Sur DC01, vérifier les événements de sécurité 4723 (tentative de changement), 4724 (réinitialisation) et 4740 (verrouillage).

8. Dépannage

Symptôme	Cause probable	Solution
« Impossible de modifier le mot de passe pour l'instant »	Règle de longueur, complexité, historique ou âge minimal non respectée	Get-ADUserResultantPasswordPolicy, expliquer les règles, ajuster l'âge minimal
Changement refusé le jour d'une réinitialisation	Âge minimal ⩾ 1 jour et case « doit changer » non cochée	Réinitialiser en cochant la case, ou PSO avec âge minimal 0
GPO de mot de passe sans effet	GPO liée à une OU et non au domaine	Lier à la racine du domaine ou utiliser une PSO
Pas de lien « Changer mon mot de passe »	login.aspx non modifié ou écrasé par une mise à jour	Ajouter le lien dans fr-FR\login.aspx
« Unable to display RD Web Access » dans Edge ou Chrome	Navigateur sans XSLT et serveur non mis à jour	Installer KB5131080 (novembre 2026) ; en attendant, stratégie XSLTEnabled = 1 ou client web HTML5

Symptôme	Cause probable	Solution
Avertissements ou boucle d'expiration sur Windows 11 22H2/23H2	Problème connu avec les DC Windows Server 2025	Mettre à jour DC et postes, tester sur Windows 11 24H2 ou plus
Avertissement de certificat	Nom ou autorité non reconnus	Certificat au nom exact, racine déployée par GPO
Compte verrouillé	Trop d'essais sur le portail	Unlock-ADAccount, vérifier l'événement 4740

9. Sécurité

- Ne jamais publier le port 3389 sur Internet. Pour un accès externe, ajouter le rôle RD Gateway (seul le port 443 est exposé) et une authentification multifacteur.
- Garder le verrouillage de compte actif : le portail web est une cible d'attaques par force brute.
- Restreindre l'accès à la collection au groupe GG_Utilisateurs_RDS.
- Appliquer chaque mois les mises à jour de RDS01 et du client web (Update-RDWebClientPackage).