Devolutions

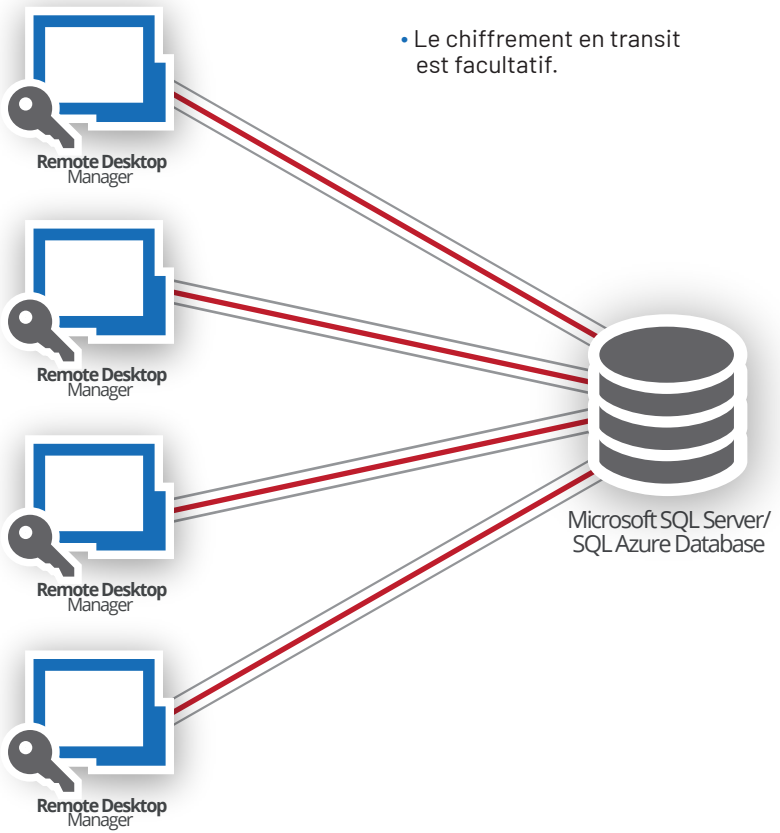
MODÈLE DE SÉCURITÉ ET CHIFFREMENT

Devolutions

Modèle de sécurité et chiffrement

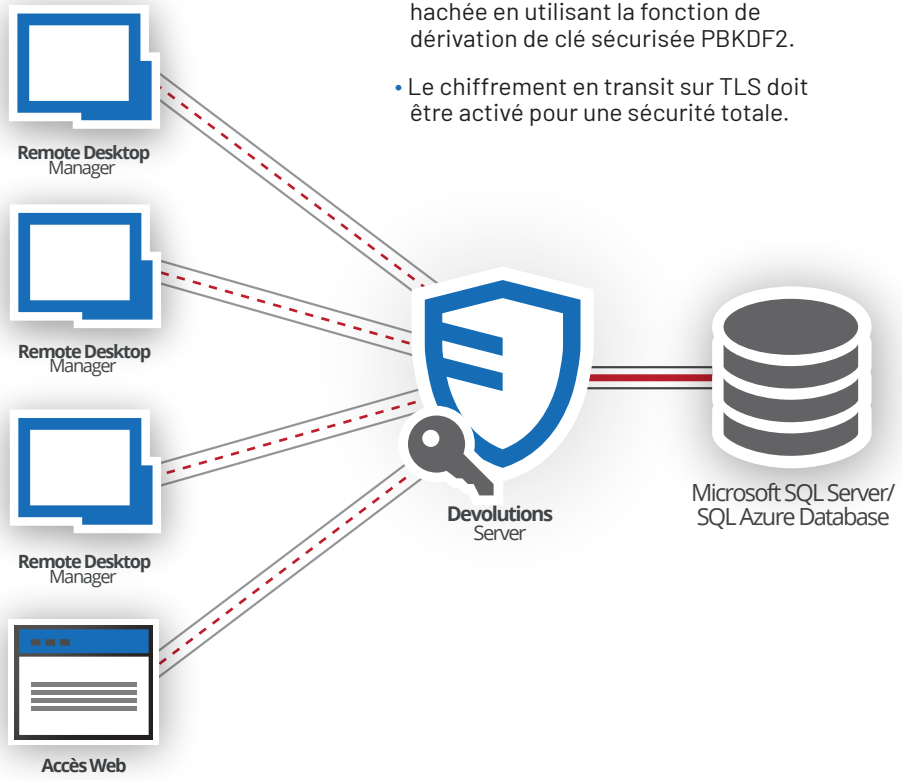
Multi-utilisateur **Remote Desktop** Manager

- Les fournisseurs de sécurité sont utilisés pour le chiffrement au repos.
- Les fournisseurs de sécurité prennent en charge les phrases secrètes et les secrets de certificats.
- Les clients doivent avoir un accès réseau à la base de données.
- Les données sont protégées par AES-256 avec des clés provenant de manière sécurisée des secrets des fournisseurs de sécurité.
- Le chiffrement en transit est facultatif.



Multi-utilisateur **Devolutions** Server

- Le chiffrement au repos est effectué par DVLS.
- Les clients ne doivent avoir qu'un accès réseau à DVLS.
- Les données sont protégées par un chiffrement sécurisé XChachaPoly1305 avec une clé générée aléatoirement à l'installation.
- Les mots de passe personnalisés des utilisateurs sont stockés sous forme hachée en utilisant la fonction de dérivation de clé sécurisée PBKDF2.
- Le chiffrement en transit sur TLS doit être activé pour une sécurité totale.



LÉGENDE : Chiffrement au repos — Chiffrement en transit ·····

Devolutions

Conformité de l'annexe A de la norme FIPS 140-2

Remote Desktop Manager version 2022.1 et ultérieure

Les fonctions de sécurité de RDM sont conformes à l'annexe A de la norme FIPS 140-2 pour le chiffrement local, le chiffrement en transit et les connexions RDP et SSH. La seule condition est que le mode d'authentification soit défini sur Mot de passe d'application et que le système sous-jacent est configuré pour utiliser la cryptographie Windows FIPS uniquement. Les autres systèmes d'exploitation, modes d'authentification et entrées de connexion ne sont pas pris en charge par le mode FIPS-only.

Les entrées de connexion qui ne sont pas prises en charge doivent être contrôlées et limitées côté serveur pour demeurer conformes.

Données (en transit)

Utilisation d'algorithmes conformes à la norme FIPS pris en charge par le système d'exploitation

MSSOL (sur TLS)
DVLS (sur TLS)

Données locales

AES-256-CBC-HMAC-SHA-256 Encrypt-then-MAC

Fichier de configuration
Cache hors ligne

Entrées prises en charge

Utilisation d'algorithmes conformes à la norme FIPS pris en charge par le système d'exploitation

RDP
TLS

Nécessite une configuration manuelle du service/serveur du système*

SSH

*Configuration SSH pour la conformité de RDM avec FIPS 140-2 :
https://kb.devolutions.net/fr/kb_ssh_configuration_rdm_fips140_2_compliance.html