Prenez connaissance de ces remarques qui facilitent l'installation de View.

Vous pouvez prendre connaissance de ces remarques dans votre langue :
Français Deutsch 简体中文 日本語 한국어

Les modifications que nous avons apportées à View 5.1 et versions supérieures requièrent de configurer les composants View un peu différemment que par le passé. Ces remarques visent à vous aider à éviter des écueils potentiels lorsque vous installez View 5.1 ou une version supérieure ou lorsque vous effectuez une mise à niveau vers cette version ou une version supérieure.

Remarque : si vous effectuez la mise à niveau à partir de View 5.1 vers une version supérieure, vous avez déjà dû effectuer ces étapes de configuration. Utilisez ces remarques pour revoir votre installation de View.

1) Vous ne pouvez pas rétrograder Serveur de connexion View 5.1 ou supérieur vers des versions précédentes.

Dans View 5.1 ou supérieur, la configuration View LDAP est cryptée et elle ne peut pas être utilisée par les versions antérieures de View.

- Après avoir mis à niveau une instance de Serveur de connexion View vers View 5.1 ou supérieur, vous ne pouvez pas rétrograder l'instance vers une version précédente.
- Après avoir mis à niveau toutes les instances de Serveur de connexion View dans un groupe répliqué, vous ne pouvez pas ajouter une autre instance qui exécute une version antérieure de View.

Remarque : la rétrogradation n'a jamais été prise en charge, mais elle fonctionnait dans les versions précédentes. Désormais, elle ne fonctionne plus.

2) Les hôtes vCenter Server et View Composer nécessitent des certificats SSL valides.

- *Meilleur choix* : Vérifiez que vCenter Server et View Composer disposent de certificats fournis par une autorité de certification (CA) :
    - Installez un certificat SSL, signé par une autorité CA, sur le serveur Windows Server sur lequel vCenter Server est installé.
    - Procédez de la même manière pour View Composer. Si vous installez View Composer et vCenter Server sur le même hôte, ils peuvent utiliser le même certificat, mais vous devez configurer le certificat séparément pour chaque composant.

      * Si vous installez le certificat avant d'installer View Composer, vous pouvez sélectionner votre certificat pendant l'installation de View Composer.

      * Si vous remplacez ensuite le certificat par défaut, exécutez la commande *SviConfig ReplaceCertificate* pour lier le nouveau certificat au port utilisé par View Composer.
    - Veillez à ce que l'autorité CA des nouveaux certificats, et les autorités CA parentes, soient autorisées par chaque serveur Windows sur lequel une instance de Serveur de connexion View est installée.

- *Alternative* : Après avoir ajouté vCenter Server et View Composer à View, acceptez l'empreinte numérique du certificat par défaut de View Composer en cliquant sur **Vérifier** dans View Administrator. Procédez de la même manière pour vCenter Server.

Plus d'informations : Consultez « Configuration de certificats SSL pour des serveurs View » dans le guide *Installation de View*.

3) Les hôtes du serveur de sécurité et de Serveur de connexion View nécessitent des certificats SSL valides.

- *Meilleur choix* : Après avoir installé une instance de Serveur de connexion View ou du serveur de sécurité sur un hôte Windows Server, ouvrez le magasin de certificats Windows Server et procédez comme suit :
    - Importez un certificat SSL signé par une autorité CA, qui peut être validé par les clients.
    - Veillez à installer l'ensemble de la chaîne de certificats, y compris les certificats intermédiaires et le certificat racine.
    - Vérifiez que le certificat dispose d'une clé privée et marquez cette clé pour indiquer qu'elle est exportable.
    - Définissez *vdm* comme nom convivial du certificat.
- *Alternative* : Laissez le programme d'installation de View Server créer un certificat par défaut dans le magasin des certificats Windows Server. Le certificat est autosigné et apparaîtra comme non valide dans View Administrator.
- *Mise à niveau vers View 5.1 ou une version supérieure* : Si les serveurs View d'origine disposent déjà de certificats SSL signés par une autorité CA, aucune action n'est nécessaire. Lors de la mise à niveau, View importe vos certificats vers le magasin de certificats Windows Server.

  Si les serveurs View d'origine disposent de certificats par défaut, mettez à niveau les serveurs View et suivez les étapes *Meilleur choix* ci-dessus.

Plus d'informations : Consultez « Configuration de certificats SSL pour des serveurs View » dans le guide *Installation de View*.

4) Les certificats de vCenter Server, View Composer et des serveurs View doivent contenir des listes de révocation de certificats (CRL).

View ne valide pas un certificat sans une liste CRL.

- *Meilleur choix* : Si nécessaire, exécutez les opérations suivantes :
    - Ajoutez une liste CRL à votre certificat.
    - Importez le certificat mis à jour dans le magasin de certificats Windows sur l'hôte de vCenter Server, de View Composer et de View Server.
- *Alternative* : Changez les paramètres de registre qui contrôlent la vérification CRL.

Plus d'informations : « Configuration de la vérification de révocation de certificat sur des certificats de serveur » dans le guide *Installation de View*.

Remarque : si votre entreprise utilise des paramètres proxy pour accéder à Internet, vous devrez peut-être configurer vos ordinateurs Serveur de connexion View pour qu'ils les utilisent. Cette étape permet de s'assurer que les serveurs peuvent accéder aux sites de vérification de révocation de certificat sur Internet. Vous pouvez utiliser les commandes *Netshell* de Microsoft pour importer les paramètres proxy dans Serveur de connexion View.

5) Le pare-feu Windows avec fonctions avancées de sécurité doit être activé sur les hôtes du serveur de sécurité et de Serveur de connexion View.

Par défaut, des règles IPsec régissent les connexions entre le Serveur de sécurité View et le Serveur de connexion View et nécessitent d'activer le pare-feu Windows avec fonctions avancées de sécurité.

- *Meilleur choix* : Réglez le pare-feu Windows avec fonctions avancées de sécurité sur **Activé** avant d'installer les serveurs View. Vérifiez que ce pare-feu est **Activé** pour les profils actifs et, de préférence, réglez-le sur **Activé** pour *tous* les profils.

- *Alternative* : Avant d'installer les serveurs de sécurité, ouvrez View Administrator et désactivez le paramètre global, *Utiliser IPsec pour les connexions au serveur de sécurité*, en lui affectant la valeur **non**. (Non recommandé.)

6) Les pare-feu principaux doivent être configurés pour prendre en charge IPsec.

S'il existe un pare-feu principal entre les serveurs de sécurité et les instances de Serveur de connexion View, vous devez configurer des règles de pare-feu pour que les connexions fonctionnent.

Plus d'informations : Consultez « Configuration d'un pare-feu principal pour prendre en charge IPsec » dans le guide *Installation de View*.

7) Les clients View Client doivent utiliser HTTPS pour se connecter à View.

Les instances de Serveur de connexion View et les serveurs de sécurité utilisent SSL pour les connexions client.

- Si les clients View se connectent via un périphérique intermédiaire de déchargement SSL, vous devez installer le certificat SSL de ce périphérique sur le Serveur de connexion View ou le serveur de sécurité.

- La connexion doit être une connexion HTTPS que les clients View se connectent ou non via un périphérique intermédiaire, tel qu'un équilibreur de charge. Si vous utilisez un périphérique intermédiaire et voulez que les connexions entre le périphérique intermédiaire et le serveur View soient établies sur HTTP (déchargement SSL), configurez le fichier *locked.properties* sur le serveur View.

- Les clients View antérieurs qui peuvent choisir de ne pas utiliser HTTPS reçoivent une erreur si les utilisateurs sélectionnent HTTP. Auparavant, ils étaient renvoyés automatiquement vers HTTPS. Les clients qui ne peuvent pas établir des connexions SSL ne peuvent pas se connecter à View.

Plus d'informations : Consultez « Déchargement des connexions SSL vers des serveurs intermédiaires » dans le guide *Administration de View*.

8) Les sauvegardes cryptées et nettoyées View nécessitent de nouvelles étapes de restauration.

Par défaut, les sauvegardes de View 5.1 ou supérieur sont cryptées. Vous pouvez également nettoyer les sauvegardes View (exclure les mots de passe et d'autres informations sensibles des données de la sauvegarde) ou effectuer les sauvegardes en clair (déconseillé).

- Pour pouvoir restaurer une sauvegarde cryptée, vous devez décrypter préalablement les données. Vous devez utiliser le mot de passe de récupération des données que vous avez fourni lors de l'installation de Serveur de connexion View.

- Ne restaurez pas les sauvegardes nettoyées. Les données, telles que les mots de passe, manqueront dans la configuration LDAP View. Les composants View ne fonctionnent pas correctement sans ces données. Pour restaurer la fonctionnalité normale, vous devez utiliser View Administrator pour réinitialiser manuellement tous les mots de passe et les autres éléments de données manquants.

Plus d'informations : Consultez « Sauvegarde et restauration des données de configuration View » dans le guide *Administration de View*.

9) Pour pouvoir mettre à niveau ou réinstaller un Serveur de sécurité View 5.1 ou supérieur, vous devez supprimer les règles IPsec appropriées de l'instance de Serveur de connexion View couplée pour pouvoir définir de nouvelles règles.

- Dans View Administrator, sélectionnez le serveur de sécurité et cliquez sur **Plus de commande > Préparer la mise à niveau ou la réinstallation**.

  Remarque : il est inutile de supprimer un serveur de sécurité depuis View avant de mettre à niveau ou de réinstaller le serveur.

Plus d'informations : Consultez « Préparer la mise à niveau ou la réinstallation d'un serveur de sécurité » dans le guide *Installation de View*.