Procédure d'installation et d'accès à la Console Sophos depuis le poste de l'administrateur de l'antivirus Sophos au niveau de l'Institution Universitaire

A. Sur le poste de l'administrateur de la solution antvirus sophos au niveau institution

1. **Télécharger** et **installer** le logiciel Sophos console 64 ou 32 bits selon le système d'exploitation de votre PC (pour télécharger la console, utiliser le mot de passe de téléchargement de la console)
2. **Créer** un compte local dédié avec les paramètres de la **console** (login et mot de passe du compte sont livrés par le CCK dans le courrier officiel -la fiche antivirus-paramètres de la console)
3. **Accèder** à l'interface Sophos console depuis le poste d'administration en ouvrant une nouvelle session **avec votre compte console et votre mot de passe console** nouvellement crée sur votre poste d'administration (voir plus de détails en bas).

B. Ouverture sur le firewall réseau de l'institution si existe

Veuillez ouvrir au niveau de votre Firewall les communications sortantes depuis vers le serveur Sophos central du CCK **Antivirus.cck.rnu.tn**.

But	Adresse IP Source	Ports Source	Adresse IP Destination	Ports Destination	Action
Accès à la console sophos Console pour suivre et administrer le parc installé de l'institution	Du poste administrateur de la solution Sophos au niveau institution et ayant installé le software SEC console	Any (all)	Serveurs CCK **Antivirus.cck.rnu.tn** 196.203.79.209	HTTP, TCP_135, TCP_DCOM : de 49152 au 65535 (intervalle de ports)	permit

Si Vous voulez, pour restreindre l'accès, nous donner l'adresse IP source (celle visible depuis Internet) du poste administrateur de la solution Sophos au niveau institution.

La procédure détaillée d'installation et d'accès vers la console Sophos sur le poste de l'administrateur antivirus au niveau de l'institution appartenant au Réseau National Universitaire RNU

Etape 1 :

Télécharger le logiciel sophos console avec votre mot de passe de téléchargement de la console indiqué dans la fiche technique antivirus, depuis le chemin http://www.rnu.tn/securite/antivirus

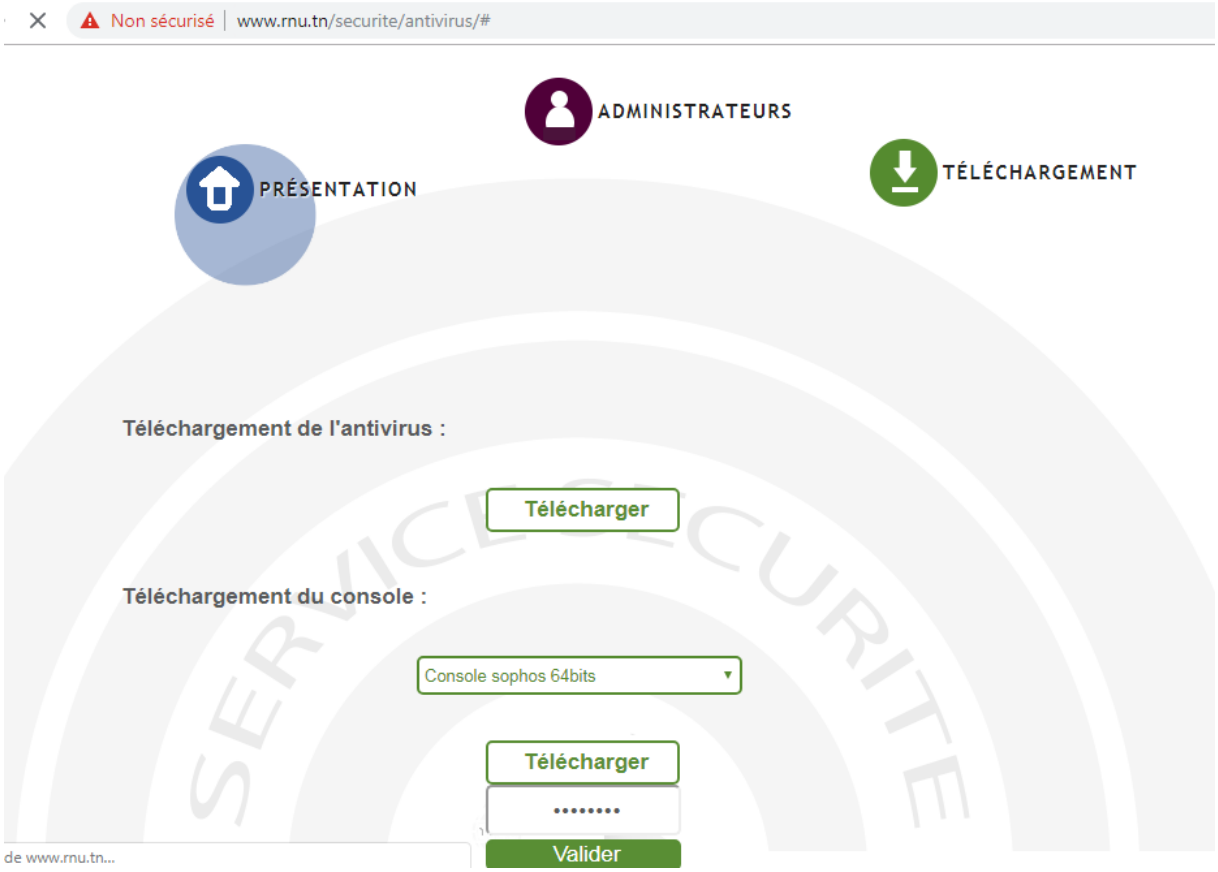
cliquer bouton TELECHARGEMENT, puis logiciels, sélectionner le système d'exploitation du poste d'administration 32 bits ou 64 bits et tapez le mot de passe de téléchargement de la console depuis votre fiche antivirus reçu par courier.

Cliquer sur l'application téléchargée et l'installer an tant administrateur du poste.

ConsoleSophos_....._x86 ou ConsoleSophos_....._x64

la taille est : 55780 KO

espace téléchargement du logiciel « console » : téléchargement/logiciels (le deuxième) choisir le système console sophos qui vous convient.

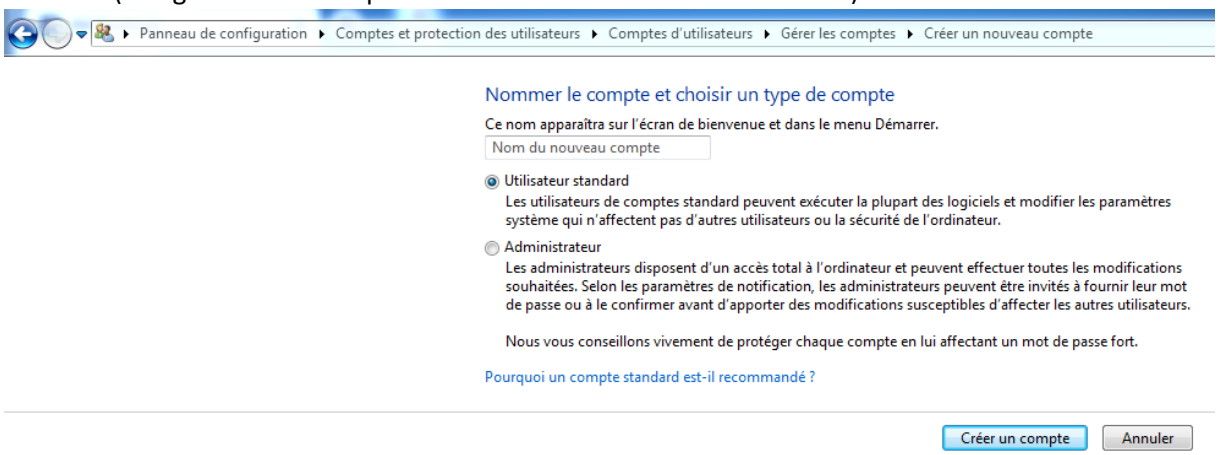


Espace documentation : Cette procédure et d'autres documents d'administration sont téléchargeables depuis : **téléchargement/procédures**

Même dans l'espace Administrateurs, il ya un résumé des étapes avec des figures.

Etape 2 :

Créer le compte Windows sur le pc d'administration de la solution antivirale: en tant que utilisateur standard (le login et le mot de passe deouis la fiche antivirus institution)



definir son mot de passe.

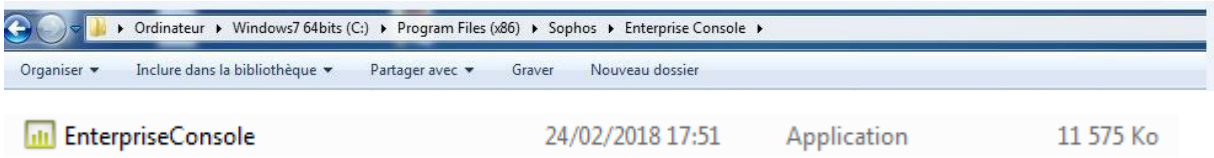
Le mot de passe désigné dans la fiche technique antivirus.

Etape 3 : Lancement et authentification sur la console avec le compte utilisateur crée localement:

1 cas : Si vous voulez ouvrir deux sessions sur le poste, vous pouvez le faire. Et donc vous ouvez la session windows avec votre compte nouvellement crée et accèder à l'application Enterpriseconsole .

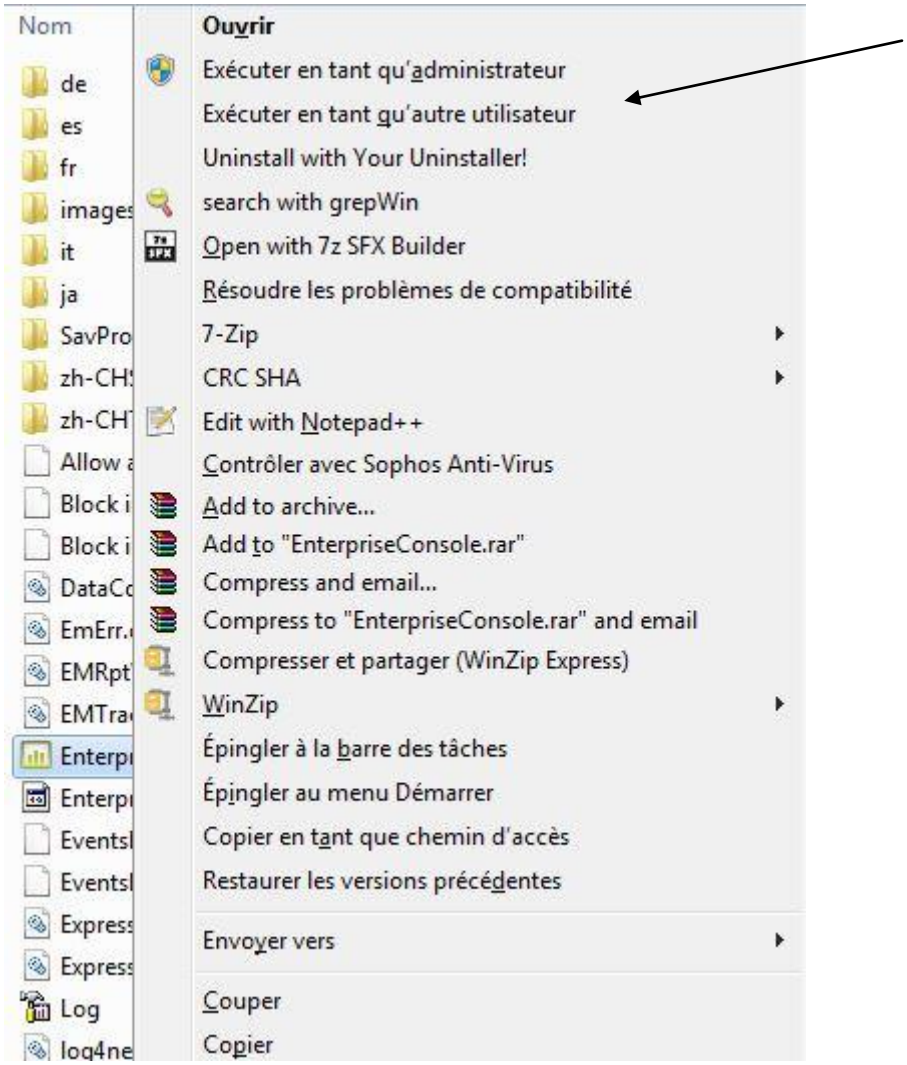
2 cas : Sinon si vous voulez garder votre session d'ouverture de session ouverte (votre compte abituel d'accès à la session windows) et en même temps vous accèder à la console pour l'adinistrer avec le nouveau compte crée :

Allez au chemin d'installation que vous avez choisie lors de l'installation, contenant le produit Entreprise console par exemple sous :

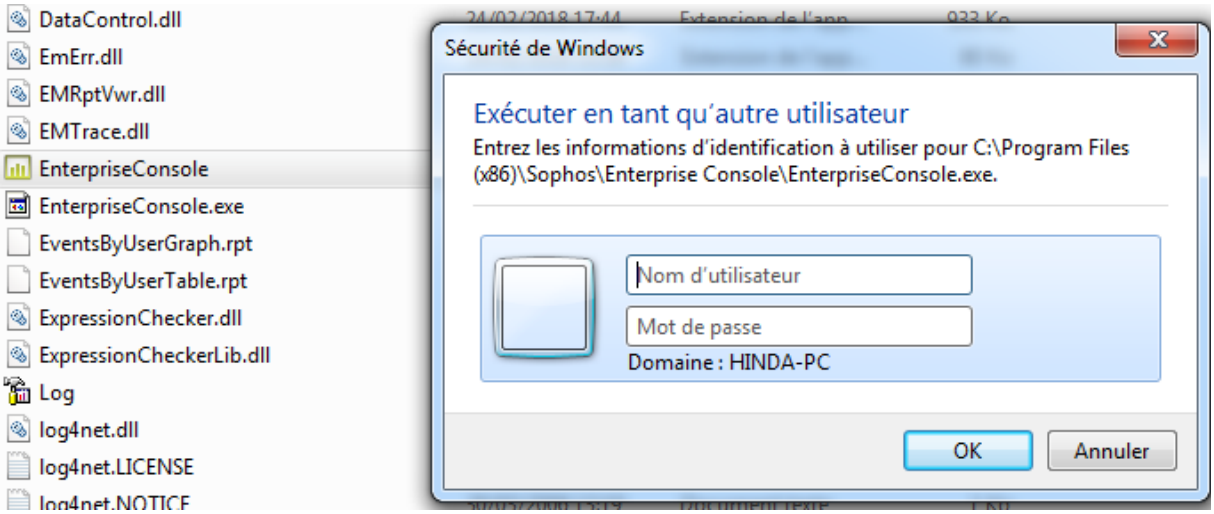


Sélectionner l'application installé EntrepriseConsole (l'icône jaune) et

Cliquer sur le shift bouton et cliquer sur le bouton droit de la souris pour afficher le menu suivant

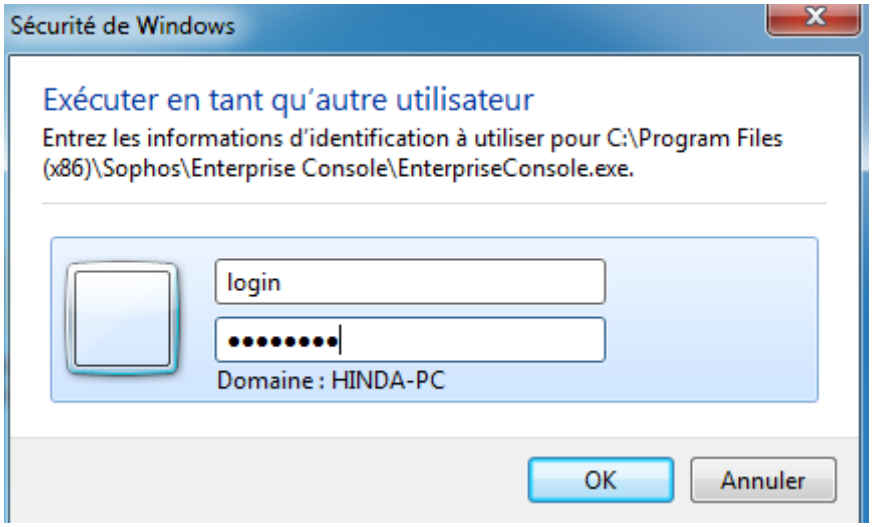


et cliquer **sur 'Exécuter en tant qu'autre utilisateur'. La fenêtre d'authentification s'ouvre.**



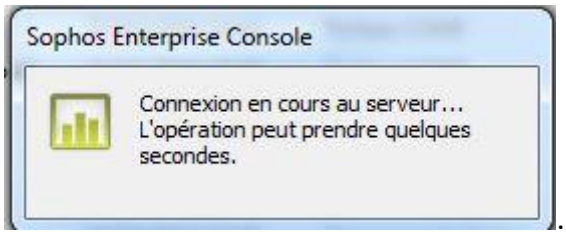
et saisir vos paramètres du compte nouvellement crée :

(login et mot de passe du compte **console** déjà crée.)



Votre domaine s'affiche au lieu de mon domaine..

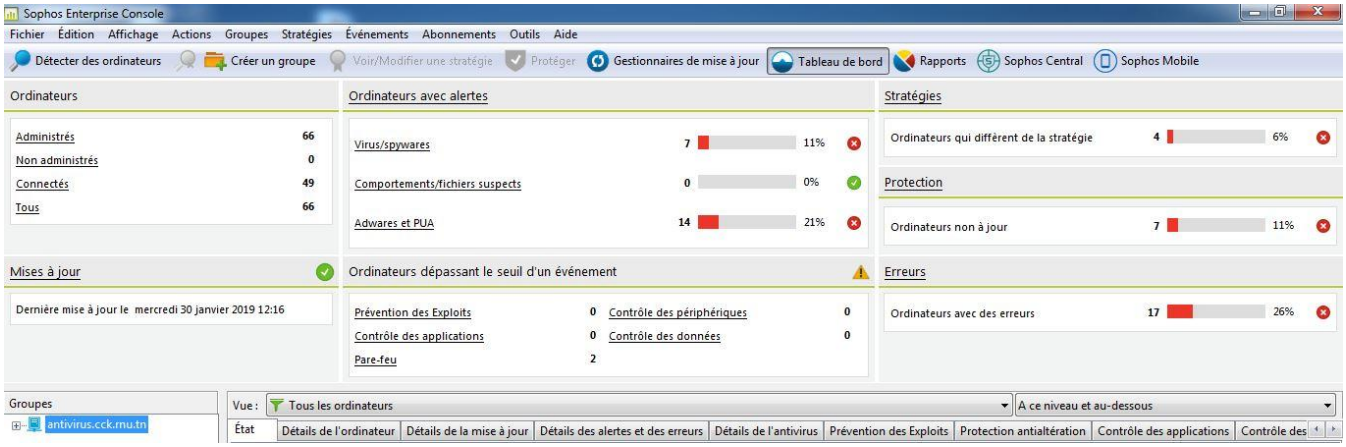
Et la console s'ouvre après un certains temps :



Comme vous pouvez créer un raccourci sur le bureau depuis le chemin d'installation pour des futurs accès.

Une fois ouverte, vous allez voire votre tableau de bord et l'interface d'administration de Sophos contenant l'état de votre parc, les groupes, la stratégie. Vous pouvez consulter els guides en lignes pour administrer.

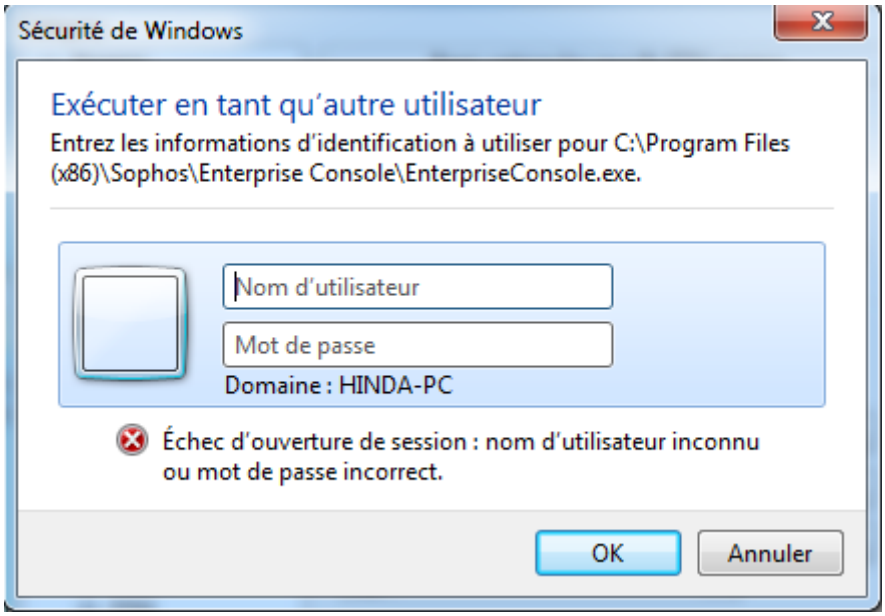
Exemple de menu qui s'affiche:



Diagnostics en cas de problème d'accès :

Les écrans suivants peuvent s'afficher :

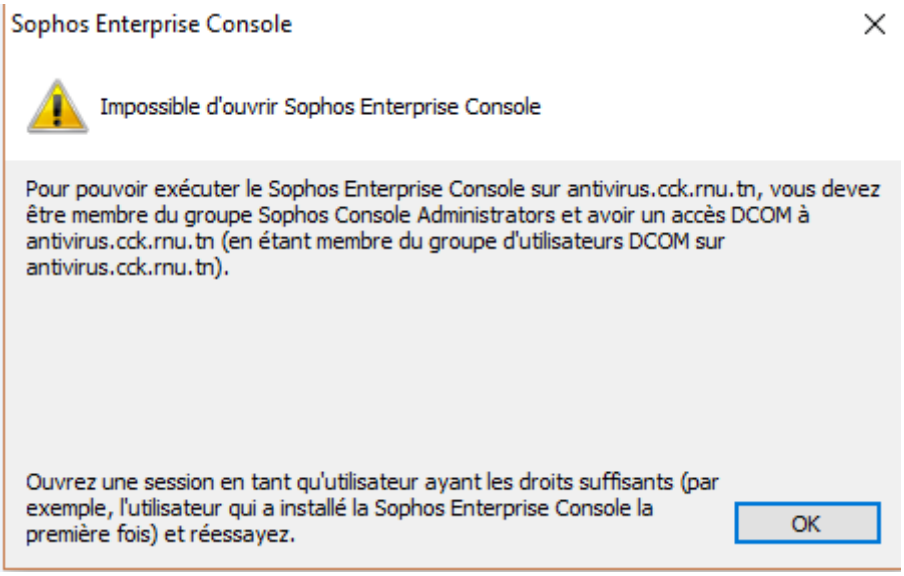
<u>Cas 1 :</u> login ou/et mot de passe non valides : suite à la saisie cet écran s'affiche



Solution 1 : vérifie que le compte est déjà crée sur le poste d'administration avec les paramètres (login et mot de passe de la console) inscrit dans la fiche antivirus.

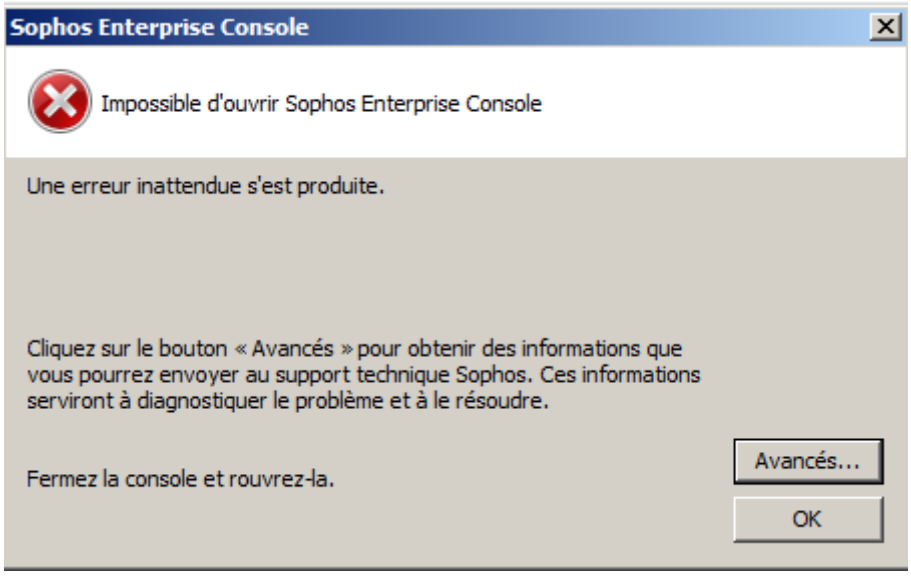
Tester l'ouverture de la session windows localement (changer utilisateur et saisir les paramètres du compte).

Cas 2 : problème de droit du compte



Solution 2 : nous contacter par émail securite@cck.rnu.tn.

Cas 3 : Problème de connectivité avec la console



Solution 3 : vérifier votre configuration du Firewall institution si existe comme décrit dans la section B dans cette procédure en haut, vérifier la connectivité du PC d'administration vers Internet et que le

serveur DNS fonctionne. Le PC d'administration doit appartenir au réseau RNU.

Vous pouvez lancer sous invite de commande DOS : cmd

Etat des connexions actives totale

C:\Users\Hinda>**netstat -na | more**

Connexions actives

Proto Adresse locale Adresse distante État

…….

…….

Etat des connexions actives au serveur antivirus

C:\Users\Hinda>**netstat -na | find "79.209"**

Proto Adresse locale Adresse distante État

TCP *VOTRE_adresseIP*:8194 196.203.79.209:53323 ESTABLISHED

TCP *VOTRE_adresse*IP:8194 196.203.79.209:61481 ESTABLISHED

TCP *VOTRE_adresse*IP:59911 196.203.79.209:8194 ESTABLISHED

TCP *VOTRE_adresse*IP:59913 196.203.79.209:8194 ESTABLISHED

C:\Users\Hinda>

a. **Connexions vers la console serveur antivirale ouvertes :**

Proto Adresse locale Adresse distante État

TCP *VOTRE_adresseIP*:8194 196.203.79.209:53323 ESTABLISHED

TCP *VOTRE_adresse*IP:8194 196.203.79.209:61481 ESTABLISHED

Vérifiez que l'état est ESTABLISHED.

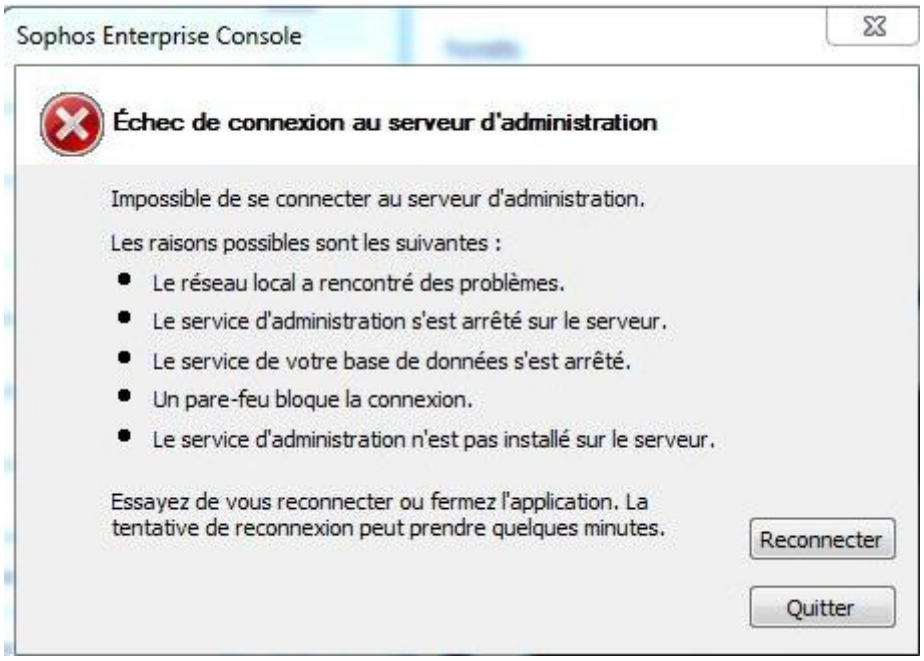
b. <u>Le Pc ce connecte pour faire la mise à jour au serveur antivirale:</u>

C:\Users\Hinda>**netstat -na | find "79.209"**

Proto	Adresse locale	Adresse distante	État
TCP	***VOTRE_adresse*IP:59911**	**196.203.79.209:8194**	**ESTABLISHED**
TCP	***VOTRE_adresse*IP:59913**	**196.203.79.209:8194**	**ESTABLISHED**

Vérifie que l'état est ESTABLISHED.

Cas 4 : Si notre server antivirale est offline/reboot



Solution4 : Nous sommes au courant et nous envoyer un émail securite@cck.rnu.tn.