



MINISTÈRE DE L'AGRICULTURE ET DE L'ALIMENTATION

MAA/SDSI

Sous-Direction des Systèmes d'Information

Rédacteurs : Thierry Deldicque, Fabrice Bertrand, Olivier Perdriel
21/11/2019

Note sur l'utilisation des solutions VPN du MAA au sein des établissements publics locaux de l'enseignement agricole

Cette note a pour objectif de définir les modalités fixées par le MAA pour l'utilisation de ses solutions VPN SSL au profit des agents employés au sein des établissements publics locaux de l'enseignement agricole.

Table des matières

1.Problématique.....	1
2.Solution proposée par le MAA.....	2
3.Modalités d'utilisation du VPN « Mercure V2 ».....	2
4.Modalités d'utilisation du VPN « Demeter ».....	2
5.Procédure de déploiement dans les EPLEFPA.....	3

1. Problématique

Le MAA a engagé en 2019 la refonte de sa solution VPN¹ SSL afin de garantir à la fois un haut niveau de sécurité de cette solution et la mise en œuvre de technologies permettant de faire face aux nouveaux besoins induits par le développement du télétravail au sein du ministère.

Le VPN « MercureV2 » succède ainsi à la solution « Mercure » dont le maintien en condition opérationnelle et de sécurité ne pouvait plus être garanti.

Les exigences de sécurité imposées par l'ANSSI pour l'homologation RGS² de « MercureV2 » ne permettent pas à un poste de travail d'accéder de manière simultanée au réseau du ministère et aux ressources hébergées sur un réseau déconnecté du réseau interministériel de l'État (RIE).

Par conséquent, avec « MercureV2 », il n'est pas possible aux agents des Établissements Publics Locaux de l'Enseignement Agricole (EPLFPA) d'accéder de façon simultanée aux applications publiées sur le RIE et à celles qui sont hébergées sur le réseau local de leur établissement (applications métier diverses, serveurs de fichiers, imprimantes...).

Cette situation obère la capacité de travail de certains agents de ces EPL qui doivent accéder fréquemment à des applications hébergées sur le RIE (en particulier RenoiRh) et accéder simultanément à des ressources hébergées sur le réseau local de leur établissement.

¹VPN : Virtual Private Network : Réseau Privé Virtuel

²RGS : Référentiel Général de Sécurité (voir sur le site de l'ANSSI

<https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/>)

2. Solution proposée par le MAA

Afin de répondre à ce besoin sans dégrader la sécurité du VPN « MercureV2 », le MAA a mis en place une seconde solution VPN qui met en œuvre un composant technique de type « Split Tunneling » permettant d'accéder à certaines ressources autorisées sur le RIE tout en maintenant l'accès aux ressources des réseaux locaux des EPLEFPA.

Cette solution VPN a été mise en service sous le nom de VPN « Demeter ».

Elle est donc réservée aux agents des EPLEFPA qui doivent accéder aux applications hébergées sur le RIE depuis leur bureau.

En aucun cas elle ne devra être utilisée en situation de nomadisme (réunion, déplacement professionnel, ...) car, pour cette utilisation, seul le VPN « MercureV2 » est homologué.

3. Modalités d'utilisation du VPN « Mercure V2 »

Le VPN « MercureV2 » est la solution VPN homologuée pour permettre l'accès au réseau du MAA et au réseau interministériel de l'état pour les agents du ministère de l'Agriculture qui se trouvent en situation de mobilité ou de télétravail.

Par extension, cette solution peut également être utilisée par certains agents des DDI ou des EPLEFPA qui se trouvent en situation de mobilité.

Son utilisation nécessite d'être en possession d'un compte « Agricoll » ainsi que d'un certificat agent valide émis par l'IGC du MAA.

Pour mémoire le certificat attribué à un agent constitue une forme de « carte d'identité numérique ». Par conséquent, un certificat est strictement personnel et ne peut donc pas être partagé.

Le déploiement du VPN « MercureV2 » a été effectué en début d'année 2019. Les communications, procédures et logiciels associés ont été envoyés vers toutes les structures dépendant du MAA (hors EPLEFPA).

En cas de besoin, les EPLEFPA sont invités à se rapprocher de leurs correspondants DRTIC ou à émettre un ticket vers le centre de service du centre de production informatique du MAA pour tout complément d'information ou pour toute demande d'assistance.

4. Modalités d'utilisation du VPN « Demeter »

Le VPN « Demeter » est la solution VPN proposée par le MAA pour permettre aux agents des EPLEFPA d'accéder à certaines applications publiées sur le RIE (Renoirh, visioconférence Jitsi, client lourd Mélanie, ...) tout en conservant les accès aux ressources informatiques hébergées au sein de leur réseau local d'établissement.

Son accès est donc autorisé uniquement depuis un poste connecté au réseau local de l'établissement.

De plus, comme pour « MercureV2 », l'utilisateur doit être en possession d'un compte « Agricoll » ainsi que d'un certificat agent valide émis par l'IGC du MAA.

Durant la phase de connexion à « Demeter », un message d'information et de mise en garde est affiché. Ce message demande à l'utilisateur de confirmer qu'il tente de se connecter au VPN depuis son établissement. La réponse à cette question est historisée. En cas de réponse négative, la connexion au VPN est interrompue.

La procédure de connexion à « Demeter » ressemble à celle de « MercureV2 ». Néanmoins elle nécessite que l'utilisateur saisisse son mot de passe « Agricoll ». De plus, avant de valider la connexion VPN, un contrôle de conformité du poste de travail est effectué automatiquement. Ce contrôle de conformité porte sur les points suivants :

- présence d'un Firewall actif sur le poste de travail
- présence d'un antivirus actif sur le poste de travail avec des bases de signature antivirales n'excédant pas 32 jours.

Si le contrôle de conformité ne satisfait pas à ces exigences, la connexion au VPN «Demeter» n'aboutira pas.

Dans ce cas, l'utilisateur est invité à se rapprocher des responsables informatiques de son établissement afin que la mise en conformité de son poste de travail soit effectuée.

5. Procédure de déploiement dans les EPLEFPA

Le client VPN permettant de se connecter à «Demeter» depuis des postes de travail MS Windows est le logiciel «Big-IP Edge Client» édité par la société F5. Il s'agit du même client que celui utilisé pour la connexion au VPN «MercureV2».

Ce logiciel a été massivement diffusé à destination des différentes structures qui sont sous la tutelle du MAA lors du déploiement de «MercureV2». Il sera également mis à la disposition des DRTIC qui assurent le lien entre le MAA et les EPLEFPA.

Les équipes informatiques de ces derniers sont donc invitées à contacter les DRTIC afin de les assister dans le déploiement du VPN «Demeter». Les DRTIC mettront à leur disposition un kit de connexion comprenant :

- le logiciel «Big-IP Edge Client» qui permet d'accéder aux VPN «Demeter» et «MercureV2»
- la procédure d'installation de ce logiciel
- deux fichiers de type «raccourcis Windows» qui pourront être déposés sur les bureaux des postes de travail Windows qui sont utilisés au sein des EPLEFPA pour accéder aux VPNs du MAA. Ces raccourcis permettront d'accéder alternativement au VPN «MercureV2» ou au VPN «Demeter»
- un fichier «Notice utilisateur VPNs EPLEFPA» permettant aux utilisateurs de distinguer les cas d'usage des VPN «Demeter» et «MercureV2».

Le Sous-Directeur des Système d'information,
Thierry Deldicque

