Formation utilisateurs à Cyberelements

Sommaire

Cahier des charges – Expression des besoins

Descriptif de l'existant

Le centre Hospitalier de Valence possède 2 systèmes d'accès à distance, le premier est **RDS Web Access** qui est intégré à Windows Server mais qui n'assure pas une forte sécurité. Le deuxième système d'accès à distance est **Cyberelements** qui agis comme une passerelle entre l'utilisateur en télétravail et la ferme RDS hébergé au centre Hospitalier, c'est un service SaaS *(Software as a Service)*.

Besoin(s)

À la suite d'un audit réalisé avec l'outil SILENE, développé par l'ANSSI, permettant d'identifier les failles exposées sur le web, l'hôpital avez besoin de sécuriser son accès à distance aux applications métiers, Cyberelements répondait au besoin en permettant l'authentification grâce à un mot de passe et un code TOTP. De plus, le système RDS Web Access nous contraignez à exposer les serveurs RDS sur Internet. Grâce à cette solution, l'utilisateur s'authentifie et se connecte via Cyberelements.

Contrainte(s)

J'ai eu 7 mois pour appeler, migrer et former chaque utilisateur qui faisait du télétravail, des astreintes ou qui ont un besoin de se connecter au DPI *(Dossier Patient Informatisé)*, comme par exemple les sages femmes libérales.

Ressources

Ressources mises à disposition

J'ai à ma disposition un ordinateur, un compte Skype Entreprise, un DECT, une adresse mail et un accès à la console AD du Centre Hospitalier de Valence.

Ressources nécessaires à la mise en place

Pour former et mettre les bons droits sur l'AD aux utilisateurs je dois avoir un ordinateur, un compte Skype Entreprise ou un DECT, une adresse mail pour les utilisateurs qui ne répondraient pas au téléphone ainsi qu'un accès à la console AD du Centre Hospitalier de Valence.

Gestion des ressources

Je vais utiliser l'ordinateur fourni par le Centre Hospitalier de Valence pour me connecter à mon compte Skype Entreprise, mon adresse mail et la console AD.

Analyse

Descriptifs des solutions

RDS Web Access est une fonctionnalité intégrée aux Remote Desktop Services (RDS) de Windows Server qui permet d'accéder à des applications ou à des bureaux distants depuis un navigateur web. Cette solution repose sur plusieurs rôles serveur comme RD Session Host, RD Gateway, RD Connection Broker et RD Web Access, qui travaillent ensemble pour fournir un accès sécurisé aux ressources internes d'une entreprise. L'utilisateur se connecte via une interface web et peut lancer des applications publiées ou un bureau distant sans installer de logiciel spécifique. L'authentification peut être intégrée à Active Directory, ce qui facilite la gestion des utilisateurs et des permissions. La sécurité peut être renforcée grâce à RD Gateway, qui encapsule les connexions RDP dans du https, permettant un accès distant sécurisé depuis Internet. Cette solution est largement utilisée dans les environnements Microsoft pour centraliser l'accès aux applications et aux postes de travail tout en simplifiant l'administration.

Cyberelements est une solution d'accès distant sécurisé conçue pour permettre aux utilisateurs de travailler à distance tout en protégeant l'infrastructure de l'entreprise. Contrairement à une solution RDS classique, Cyberelements repose sur une architecture de cyber-isolation, où l'utilisateur accède à un environnement sécurisé intermédiaire plutôt qu'au système interne directement. Cette approche réduit considérablement les risques liés aux attaques ou aux compromissions des postes clients. La solution intègre différentes fonctionnalités de sécurité comme le contrôle des postes et la connexion par code TOTP. Elle est pensée pour fonctionner avec différents systèmes et environnements IT, et vise particulièrement les organisations qui doivent sécuriser fortement les accès distants, notamment dans des contextes sensibles ou réglementés.

Comparaison des solutions (tableau)

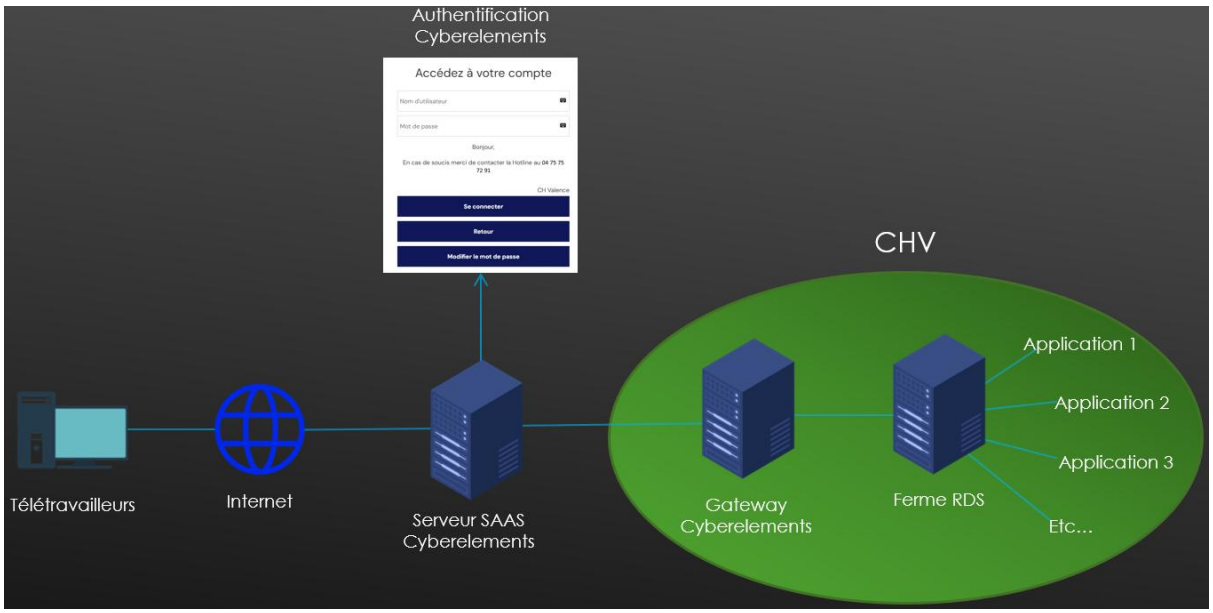
Critères \ Solutions	RDS Web Access	Cyberelements
Fonctionnement	Connection sur la ferme RDS en direct.	Connection sur un portail sécurisé avant d'accéder aux applications hébergées sur la ferme RDS.
Méthode d'authentification	Basique : identifiant et mot de passe.	Elevé : identifiant, mot de passe, code TOTP et vérification de l'ordinateur.
Coûts	Licence Windows Server.	Licence Windows Server et licence Cyberelements.
Accès	Accès aux applications après une authentification simple.	Accès aux applications après une authentification forte.
Exposition	Exposition de la ferme RDS sur Internet.	Ferme RDS protégé par Cyberelements.

Choix d'une solution - Argumentation

Le centre hospitalier de Valence a choisi Cyberelements car il permet de ne pas exposer la ferme RDS directement sur Internet. De plus, Cyberelements ajoute une couche de sécurité en demandant un code TOTP.

Plan d'adressage - Schéma - Tables de routage

Le Centre Hospitalier de Valence est un établissement de santé public, je ne suis pas autorisé à expliquer la configuration réseau.
Cependant, vous trouverez ci-dessous un schéma expliquant simplement comment un utilisateur peut se connecter à la ferme RDS depuis l'extérieur.



Étude de l'impact sur le SI existant

L'intégration de **Cyberelements** dans une infrastructure informatique permet de sécuriser les accès distants des utilisateurs et de faciliter le télétravail. Cette solution repose sur une approche **Zero Trust**, qui consiste à vérifier systématiquement l'identité de l'utilisateur et l'état du poste avant d'autoriser l'accès aux ressources du système d'information. Elle améliore la sécurité globale du SI tout en permettant aux utilisateurs d'accéder à leurs applications et services depuis l'extérieur.

- **Impact technique :**

La mise en place de Cyberelements nécessite l'intégration d'une plateforme d'accès distant sécurisée entre les utilisateurs externes et les ressources internes du système d'information. Les connexions passent par un portail sécurisé qui contrôle l'identité de l'utilisateur, l'état du poste utilisateurs et les droits d'accès avant d'autoriser la connexion aux applications internes.

La solution s'appuie sur une architecture **Zero Trust Network Access (ZTNA)** qui limite les accès aux seules ressources autorisées et applique le principe du moindre privilège. Elle permet également d'intégrer des mécanismes d'authentification forte, de contrôle de conformité des postes et de gestion centralisée des accès.
Cette intégration implique donc une configuration précise des identités, des règles d'accès, des applications publiées et des mécanismes d'authentification. Elle nécessite également une bonne intégration avec les systèmes existants tels que l'Active Directory (AD).

- **Impact organisationnel :**

L'arrivée d'une solution de télétravail sécurisée modifie l'organisation des accès au système d'information. Les utilisateurs ne se connectent plus directement au réseau interne mais passent par une plateforme centralisée qui contrôle et journalise leurs accès. L'équipe informatique doit mettre en place de nouvelles procédures pour la gestion des accès distants et la configuration du client Cyberelements.

- **Impact stratégique :**

Cyberelements renforce la stratégie de sécurisation du télétravail en remplaçant une logique de confiance par une logique Zero Trust fondée sur l'identité, le contexte et le cloisonnement. Elle améliore également la sécurité des accès externes en évitant l'exposition directe des services internes sur Internet. Cette approche permet de réduire la surface d'attaque du système d'information.

- **Impact humain :**

La mise en place de cette solution nécessite une adaptation des utilisateurs et des équipes informatiques. Les utilisateurs doivent apprendre à utiliser une authentification forte par code TOTP pour se connecter aux applications métiers. Cela implique que chaque utilisateur dispose d'un appareil mobile compatible et soit en mesure de l'utiliser au moment de la connexion. Pour l'équipe informatique, cela génère une charge supplémentaire liée à l'enrôlement des comptes et à l'assistance en cas de perte d'accès au code TOTP (perte du téléphone, réinstallation, etc.).

- **Impact juridique :**

L'accès distant au système d'information implique la manipulation de données potentiellement sensibles depuis l'extérieur de l'organisation. La solution Cyberelements contribue à répondre aux exigences de sécurité en matière de protection des données grâce à l'authentification forte, au contrôle des postes de travail et à la traçabilité des accès.
Les connexions et les actions des utilisateurs peuvent être enregistrées et analysées afin de répondre aux exigences d'audit, de conformité et de sécurité. Ces journaux doivent être conservés conformément aux politiques internes de sécurité et aux obligations réglementaires, notamment celles liées à la protection des données personnelles.

Phasage de l'intervention

Afin de savoir qui je devais former, un collègue avait mis en place un script qui lister dans un fichier Excel, tous les jours à minuit, les utilisateurs s'étant connecté dans la journée à la

ferme RDS sans passer par Cyberelements. Grâce à cela j'ai pu créer une liste d'environ 150 utilisateurs.

Prévision des tests de validation

Avant d'appeler les utilisateurs, j'ai réalisé des tests sur un compte Active Directory dédié afin de comprendre le rôle de chaque groupe AD lié à Cyberelements.

Lors des appels pour former les utilisateurs, j'ai adapté mon approche selon les profils : certains utilisateurs se sont appuyés sur les procédures fournies pour effectuer les manipulations en autonomie, tandis que pour d'autres, j'ai pris le temps de les accompagner pas à pas dans la réalisation des différentes étapes.

Mise en place

Vous trouverez ci-dessous le lien pour accéder à la procédure donnée aux utilisateurs du Centre Hospitalier de Valence qui, pour des raisons de confidentialité, a été modifié :
https://www.mathys-demon.fr/wp-content/uploads/2026/03/Teletravail-Procedure-utilisateurs-connexion-et-configuration-Cyberelements.pdf

Le projet arrivant à son terme, j'ai formé les équipes du support informatique ainsi que les personnes d'astreinte afin d'assurer la transition vers un fonctionnement en mode routine. Cette passation leur a permis de prendre le relai en toute autonomie, en s'appuyant sur les procédures que j'avais rédigées.

Bilan

Conclusion

Ce projet s'est déroulé de manière satisfaisante et a permis de répondre pleinement au besoin initial. La transition vers la nouvelle plateforme d'accès à distance s'est faite efficacement, et les utilisateurs ont été correctement formés.

Auto-évaluation

Ce projet m'a permis de renforcer ma confiance en moi grâce aux centaines d'appels utilisateurs. Il m'a également permis d'améliorer mon organisation en mettant en place un suivi rigoureux grâce à Excel, recensant les utilisateurs à contacter, ceux déjà joints, les personnes injoignables, les rappels à effectuer ainsi que les éventuels incidents rencontrés.

Tout au long de ce projet, j'ai effectué des points hebdomadaires avec mon tuteur afin de faire le bilan des avancées et d'ajuster ma méthode de travail. Ces échanges ont été bénéfiques à plusieurs niveaux : mon tuteur m'a orienté sur la méthode à adopter pour les appels et la formation des utilisateurs, et m'a encouragé à contacter activement les

utilisateurs. Il me faisait également des retours sur les livrables que je produisais, notamment les procédures. Selon les cas, il validait mon travail ou me demandait des corrections et des améliorations, ce qui m'a permis de progresser et d'affiner mes productions au fil du projet. Ce suivi régulier a largement contribué à la réussite et au bon déroulement de ce projet.