



IPdiva Cleanroom

Un poste de travail administrateur totalement
dédié, stérile et contrôlé !

Systancia IPdiva Cleanroom

- > Mise à disposition d'un poste administrateur virtualisé totalement stérile et à usage unique
- > Environnement dédié aux fonctions critiques de l'administrateur, dissocié de son environnement habituel
- > Renforcement des connexions aux ressources administrateurs et de la politique de mots de passe basé sur la technologie SSO
- > Surveillance en temps réel des actions menées par l'administrateur sur les ressources critiques
- > Alertes paramétrables avec déclenchement d'actions conservatoires en cas d'actions non autorisées ou malveillantes
- > Solution répondant aux attentes de mobilité sécurisée des administrateurs

Répondre aux exigences croissantes de sécurité des postes administrateurs

La sécurité des systèmes d'information repose aujourd'hui fortement sur les utilisateurs à privilèges. Un administrateur informatique, interne ou externe, dispose de prérogatives fortes sur les ressources critiques de l'entreprise. La pratique courante voulant qu'il utilise son poste de travail pour exercer aussi bien ses missions critiques que consulter un site internet est un risque fort pour l'entreprise. Le premier danger concerne la contagion d'une menace virale ou malveillante parvenue par son environnement le moins protégé (messagerie personnelle, travaux de bureautique, etc...). Le second est lié aux fonctions d'administration qui ont un impact majeur pour l'entreprise et doivent être exécutées dans un environnement spécifique où l'administrateur a conscience que chaque geste est engageant. Par ailleurs, autant il est réaliste de s'assurer de la sécurité d'un poste cloisonné et dédié, autant il est plus difficile de s'en assurer pour un administrateur opérant ses missions depuis un poste banalisé.

Il en ressort que le poste de travail de l'administrateur doit être dédié et complètement étanche. D'ailleurs, dans les arrêtés fixant les règles de sécurité relatives aux SI des opérateurs d'importance vitale, il est précisé que les opérations d'administration doivent s'effectuer sur des postes dédiés et qu'un compte d'administration ne doit servir qu'à l'administration, pratique également très fortement recommandée par l'ANSSI. Le contrôle d'un environnement à privilèges est devenu aujourd'hui incontournable pour tracer les actions réalisées afin de stopper le plus rapidement possible toute action maladroite ou malveillante. L'objectif est également en cas d'intrusion de pouvoir comprendre ce qui s'est passé. Autant la surveillance d'un environnement où l'utilisateur mixerait ses activités critiques d'administration et tâches classiques paraît difficile pour des raisons de confidentialité et de volume d'informations, autant **ce contrôle doit s'imposer pour cet environnement dédié.**

C'est la raison pour laquelle Systancia, seul acteur présent sur le marché du VDI (Virtualisation Desktop Infrastructure) et du PAM (Privileged Access Management), a eu l'idée d'associer les performances, l'agilité de la mise à disposition de postes de travail virtualisés et la sécurité apportée par les mécanismes de surveillance d'utilisateurs à pouvoirs. Ainsi est née IPdiva Cleanroom, seule solution globale du marché répondant aux exigences de sécurité croissantes des postes de travail administrateurs.

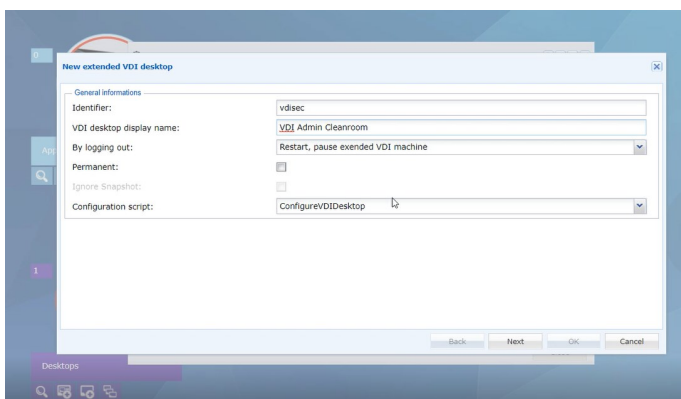
Tel. +33 (0)3 89 33 58 20

www.systancia.com



Mise à disposition d'un poste administrateur virtualisé

IPdiva Cleanroom repose tout d'abord sur les performances et l'agilité de la mise à disposition de postes de travail virtualisés (VDI). La solution intègre les fonctionnalités VDI d'AppliDis Fusion, solution reconnue pour la virtualisation d'applications et postes de travail. IPdiva Cleanroom permet de virtualiser le système d'exploitation du poste de travail dans son ensemble. Les différents postes virtuels ou physiques sont hébergés dans un data-center sécurisé pour une meilleure disponibilité et une sécurité accrue des données. L'administrateur



utilise son poste par accès distant et déport d'affichage, comme s'il était présent localement sur son poste. L'environnement de travail de l'administrateur est donc totalement étanche avec des fonctionnalités avancées renforçant la sécurité comme l'interdiction du copier-coller, l'isolation des périphériques, etc...

IPdiva Cleanroom offre des fonctionnalités de gestion dynamique du cycle de vie du clone VDI, en permettant de provisionner des postes administrateurs à la volée qui peuvent ensuite être automatiquement supprimés. Le poste de travail administrateur peut ainsi être permanent (il conserve le même environnement de travail d'une connexion à l'autre) ou peut être à usage unique, c'est-à-dire renouvelé à chaque connexion de l'administrateur.

IPdiva Cleanroom permet également de banaliser les postes de travail VDI, par exemple en les définissant par métier afin qu'ils soient identiques pour chaque membre du groupe métier correspondant.

Renforcement des connexions aux ressources et de la politique de mots de passe

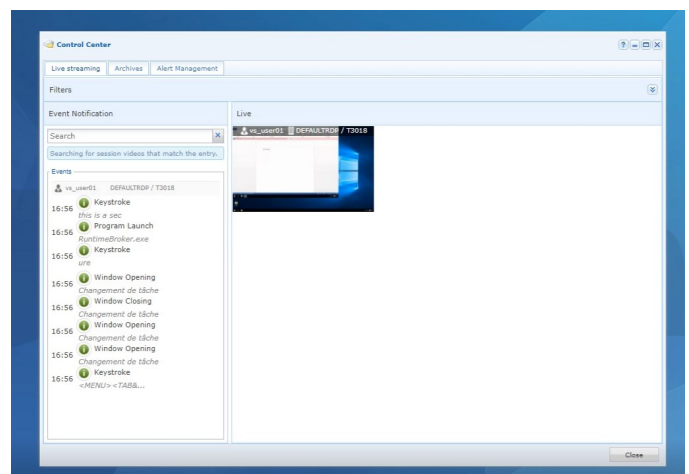
A partir de cet environnement, l'accès aux ressources protégées est réalisé avec des authentifications pour lesquelles le mot de passe n'est jamais dévoilé à l'administrateur. IPdiva Cleanroom intègre des fonctionnalités de coffre-fort de mot de passe, c'est-à-dire un bunker numérique stockant l'ensemble des logins/mots de passe en lien avec les ressources auxquelles l'administrateur a le droit d'accéder. Ce bunker numérique est un composant de la solution Avencis SSOX, solution d'authentification SSO de Systancia ayant obtenu le label France Cybersecurity.

La fonction authentification SSO automatise l'authentification aux ressources administrateurs après saisie des moyens de connexions primaires.

Le coffre-fort de mots de passe permet de gérer le cycle de vie des mots de passe ainsi que leur complexité renforçant ainsi la mise en place de la politique de sécurité des systèmes d'information au sein de l'entreprise.

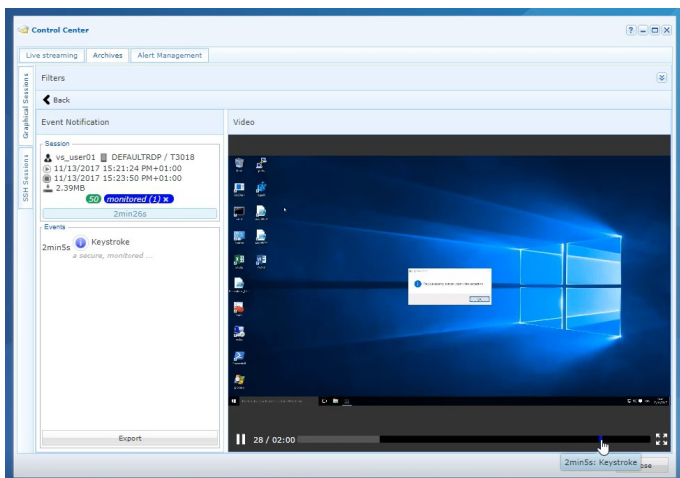
Surveillance des actions menées par l'administrateur sur les ressources

IPdiva Cleanroom permet l'enregistrement vidéo des sessions utilisateurs avec une fonctionnalité de live streaming pour visionner en temps réel les actions menées par l'administrateur sur le système d'information. Il est ainsi possible de réagir en temps réel en cas de problème détecté, en décidant de suspendre ou encore d'interrompre la session de l'administrateur.



IPdiva Cleanroom permet une analyse très fine du comportement des utilisateurs en identifiant tous les événements sur un système cible (frappe clavier, lancement d'application, lancement de processus...).

Il est ainsi possible de paramétrer des alertes afin que soit



identifiée et remontée toute action non autorisée. IPdiva Cleanroom permet également de définir des actions conservatoires qui seront déclenchées automatiquement en cas de notification d'une alerte, comme par exemple, la fermeture immédiate de la session de l'administrateur.

Par ailleurs, une fonctionnalité Archives centralise toutes les vidéos qui ont déjà été enregistrées. En une vue l'administrateur peut voir les vidéos enregistrées le jour même ou les jours précédents et pour chaque vidéo il dispose d'informations synthétiques. IPdiva Cleanroom permet également de chercher une information précise parmi plusieurs centaines d'heures de vidéos, et donc plusieurs dizaines de Téra octets de données. Ces fonctions de recherche se basent sur un moteur de recherche intelligent qui permet de lancer des recherches texte mais également sur des actions ou

des événements en garantissant la performance de la recherche et l'obtention de résultats en temps réel.

Une solution répondant aux attentes de mobilité sécurisée de l'administrateur

IPdiva Cleanroom est une solution qui répond aux attentes des administrateurs en matière de mobilité contrairement à de nombreuses solutions qui vont les confiner au sein de l'entreprise. Ainsi l'administrateur va pouvoir accéder à l'environnement d'administration depuis l'extérieur de l'entreprise.

IPdiva Cleanroom permet de donner un accès sécurisé aux ressources choisies du système d'information pour les administrateurs nomades ou les tiers-mainteneurs. Basé sur un système à double barrière, IPdiva Cleanroom propose un accès unique ne nécessitant pas l'ouverture de port sur le Système d'Information (un seul flux sortant).

Par ailleurs, des fonctionnalités avancées en matière de sécurité des accès assurent un contrôle de conformité (intégrité et sécurité) des postes distants qui se connectent aux ressources internes. Ce contrôle de conformité ou non-conformité pourra occasionner soit le rejet complet de l'accès, soit des restrictions quant aux différents niveaux d'accès souhaités. La solution propose également des fonctionnalités permettant de définir des règles d'accès en fonction de plages horaires, de sites autorisés....

IPdiva Cleanroom s'appuie sur le moteur de IPdiva Secure, seule solution ayant obtenu la qualification – niveau élémentaire délivrée par l'ANSSI dans le domaine technique « identification, authentification et contrôle d'accès ».

Fonctionnalités principales

- > Mise à disposition d'un poste de travail virtualisé
- > Fonctionnalités avancées garantissant l'étanchéité du poste de travail virtualisé : interdiction du copier/coller, isolation des périphériques...
- > Provisioning de postes administrateurs à la volée qui peuvent ensuite être automatiquement supprimés
- > Possibilité de définir des masters VDI administrateur par métier et ainsi de banaliser le poste VDI pour les membres d'un même groupe métier.
- > Authentification SSO automatisant l'authentification aux ressources administrateur après saisie des moyens de connexions primaires
- > Coffre-fort de mots de passe permettant de gérer le cycle de vie des mots de passe ainsi que leur complexité
- > Enregistrement au format vidéo de la session administrateur

> Visualisation live des sessions en cours et visualisation complète des sessions finalisées

> Paramétrage d'alertes déclenchant, en cas de suspicion de malveillance, des actions automatiques comme la fermeture de la session

> Recherches transverses par mot clé et positionnement des événements sur la timeline de la vidéo enregistrée

> Traçabilité étendue

> Accès distant sécurisé via un seul flux sortant, sans ouverture de ports sur le SI

> Accès sélectif et contrôlé aux ressources administrateurs autorisées

> Contrôle de conformité et intégrité des postes administrateurs

A propos de Systancia

Systancia est un acteur européen reconnu sur les marchés de la virtualisation, de la cybersécurité et de la confiance numérique, proposant la nouvelle génération d'infrastructure de mise à disposition des applications centrée sur la sécurité et les utilisateurs: solutions de virtualisation d'applications et VDI, de sécurité des accès externes, de surveillance des utilisateurs à pouvoirs (PAM), d'authentification unifiée (SSO) et de gestion des identités (IAM).

Misant sur l'innovation comme moteur de croissance, Systancia s'appuie sur la valeur technologique de ses produits et la proximité entre ses équipes et ses clients pour répondre aux besoins des utilisateurs et ainsi atteindre 98 % de satisfaction clients.

Systancia bénéficie d'une véritable reconnaissance comme en témoigne la Qualification – Niveau élémentaire délivrée par l'ANSSI à sa solution de cybersécurité, qui en fait la seule solution de sa catégorie à être recommandée par cette autorité nationale pour la sécurité des SI.

www.systancia.com