



APERÇU DE LA SÉCURITÉ CLOUD DE LABSTATS

LabStats est un progiciel qui collecte des données sur l'utilisation du matériel et des logiciels et qui offre des statistiques d'utilisation et des analyses de données sur cet usage aux utilisateurs autorisés via le Portail LabStats. Certaines portions du progiciel LabStats peuvent être hébergées sur le cloud et cet Aperçu de Sécurité & Conformité fournit les détails de cet arrangement.

Fournisseur de Services

LabStats utilise la plateforme cloud de Microsoft Azure pour fournir le produit LabStats sur le cloud. Cette plateforme d'une très haute fiabilité a été choisie pour différentes raisons, y compris : son historique de plusieurs dizaines d'années en tant que fournisseur de solutions logicielles, sa reconnaissance par l'industrie comme étant le premier fournisseur de plateformes cloud, sa sécurité et sa limitation des risques de classe mondiale, ses offres à haute disponibilité, et parce qu'ils ont les certifications et attestations les plus conformes de tous les fournisseurs cloud.

Données collectées

Matériel

LabStats collecte des informations uniquement sur les ordinateurs spécifiés, et inclut, à l'heure actuelle, des informations telles que le fabricant, le modèle, le numéro de série, le nom de l'hôtel, système d'exploitation, détails du processeur, détails de la mémoire, adresses IP, adresses MAC, détails de la carte graphique, la disponibilité/capacité du disque dur. Les valeurs du nom de l'hôte peuvent être remplacées manuellement afin d'obscurcir l'identité de certains ou de tous les ordinateurs.

Utilisation du matériel

LabStats collecte les informations relatives à l'utilisation uniquement sur les ordinateurs spécifiés, telles que le moment où l'ordinateur est allumé et éteint et les connexions et déconnexions à l'ordinateur et par quels comptes d'utilisateurs.

Applications

LabStats collecte des informations relatives uniquement aux logiciels installés sur et/ou utilisés depuis les ordinateurs spécifiés, et à l'heure actuelle inclut des informations telles que le nom, le pattern de nom de processus pour les applications de bureau et le pattern d'URL pour les

applications web. Les valeurs de nom de l'application peuvent être remplacées manuellement afin d'obscurcir l'identité de certaines ou de toutes les applications.

Utilisation des applications

LabStats collecte des informations relatives uniquement aux logiciels spécifiés installés sur et/ou utilisés depuis les ordinateurs spécifiés, telles que à quel moment l'application a été lancée et fermée et par quel compte utilisateur ainsi que la durée pendant laquelle elle était active.

Comptes utilisateurs

LabStats collecte des informations de tous les comptes utilisateurs utilisés pour se connecter aux ordinateurs spécifiés, et à l'heure actuelle inclut des informations telles que le nom d'utilisateur. Les valeurs de nom d'utilisateur peuvent être remplacées manuellement afin d'obscurcir l'identité de certains ou de tous les comptes utilisateurs.

Accès aux données

Utilisateurs autorisés

Votre structure est responsable de l'accès donné au Portail LabStats et les données qu'il contient. Ainsi, votre structure décide de qui doit avoir accès et du niveau d'accès. Votre structure a, en permanence, l'entier contrôle de cet accès et peut apporter des changements au besoin, avec effet immédiat.

Employés de LabStats

Autant que nécessaire pour accomplir leurs fonctions et vous soutenir dans votre utilisation du produit LabStats, certains employés de LabStats peuvent avoir un certain niveau d'accès à vos données, y compris les employés du service client, du service assistance et du service développement de logiciels. L'accès est limité, ponctuel et n'est accordé qu'aux employés nécessaires et qui ont été formellement évalués et qui ont signé des accords de confidentialité et non divulgation.

Accès brut

Tant que l'abonnement est actif, les Utilisateurs autorisés ont accès aux données au sein du Portail LabStats, cependant, vous pouvez également demander l'accès à vos données brutes périodiquement afin de faciliter toute sauvegarde secondaire, audit ou autres besoins.

Politiques relatives aux données

Propriété

Votre structure conserve la propriété des données collectées par LabStats. LabStats maintient une licence pour l'utilisation de ces données dans le but de fournir à votre structure des statistiques et analyses d'utilisation.

Stockage

Les données collectées par LabStats sont stockées sur le centre de données cloud le plus proche de votre emplacement physique dans lequel LabStats maintient une présence, ce qui inclut actuellement des centres de données aux États-Unis (Californie), aux Pays-Bas et à Singapour. Si votre structure ne réside pas dans l'un de ces pays, vous pouvez contacter le support LabStats pour découvrir dans quel centre de données vos données sont ou seraient stockées.

Rétention

Les données collectées par LabStats sont conservées tant qu'un abonnement actif est maintenu et leur destruction est programmée à l'expiration de l'abonnement. À l'issue d'une petite période suivant l'expiration de l'abonnement et sauf indication contraire, la source principale de données est enregistrée et l'original est détruit. La sauvegarde est maintenue dans le cloud mais sera hors ligne pendant une autre période de temps et peut être restaurée dans l'hypothèse où vous souhaitez rétablir votre compte. À l'issue de cette période, votre sauvegarde de données est détruite définitivement et ne peut pas être retrouvée.

Accès au système

Ordinateurs

Le client LabStats est installé sur des ordinateurs physiques ou virtuels spécifiés, la plupart du temps au sein du réseau de votre structure. Ce client fonctionne avec des privilèges standards et bas, et est demandé pour la collecte de données (tel que souligné dans Données collectées).

Active Directory

L'intégration dans Active Directory est optionnelle et permet aux ordinateurs d'être automatiquement organisés en groupes dans LabStats ce qui mimique l'organisation dans Active Directory. L'intégration peut également être utilisée pour collecter le nom d'affichage du compte d'utilisateur au lieu du nom d'utilisateur. Ces deux options d'intégration peuvent être choisies de manière indépendante. L'accès à l'Active Directory est réalisé par l'application LabStats via un compte avec autorisation de lecture seule et peut être révoqué à tout moment ; l'autorisation peut être limitée à un sous-ensemble de OUs. Les identifiants de comptes sont cryptés et ne peuvent pas être vus par les utilisateurs du Portail ou les employés de LabStats. La connexion au serveur AD se fait à travers le port 389 utilisant la bibliothèque « Services Directory ».NET créée par défaut par Microsoft, cependant, si le serveur AD supporte des connexions SSL, le port 636 peut être utilisé à la place pour établir une connexion sécurisée.

Active Directory Azure

L'intégration avec le Active Directory Azure est optionnelle et permet aux utilisateurs du Portail LabStats de se connecter en utilisant le compte fourni par leur structure, place le contrôle des accès à LabStats et ses données dans les mains de votre département informatique ou sécurité et applique vos mots de passe et politiques de sécurité sur le Portail LabStats. Les mots de passe d'utilisateurs ne sont pas partagés avec LabStats et l'authentification est gérée par Microsoft.

Sécurité

Physique & numérique

Pour ses offres cloud, LabStats utilise les centres de données de Microsoft Azure qui mettent en place de nombreuses mesures pour protéger les opérations et les données de menaces ou d'intrusions physiques ou virtuelles. Les centres de données sont conformes aux standards du marché (tels que ISO 27001) concernant la sécurité physique et la disponibilité. La sécurité des centres de données est endurcie et leurs emplacements ne sont pas publiés. Ils bénéficient de la mise en place d'un important système de sécurité physique, incluant une clôture de périmètre, des caméras de surveillance, un personnel de sécurité, des accès sécurisés, des réseaux de communications en temps réel, etc.

Les données en transit

Les données transmises à et depuis le Portail LabStats et le Service Client LabStats (API) sont cryptées via l'utilisation d'un protocole TLS 1.2 certificat SSL avec un cryptage 2048 bits SHA-256 bits. Les certificats sont constamment mis à jour afin qu'ils n'expirent jamais.

Les données au repos

Certaines données sensibles sont cryptées au repos pour une couche de sécurité supplémentaire en utilisant un cryptage AES de 256 bits avec un mot de passe privé et salage. Le cryptage est réversible par le Portail LabStats, tel que cela est requis, afin de présenter les données aux utilisateurs autorisés du portail ou pour authentifier les actifs du réseau intégré (dans l'hypothèse d'une intégration avec Active Directory).

Isolement

Les données sont stockées en isolement via des bases de données séparées et elles ne sont pas mélangées avec les données d'une autre structure. L'accès d'une base de données à une autre est intrinsèquement interdit.

Exécution du code

Le Portail LabStats et ses systèmes de support sont développés et déployés avec un contrôle de sécurité élevé. L'application est précompilée, examinée par des pairs et est développée en utilisant des standards stricts de contrôle afin qu'aucun code non autorisé ne soit autorisé à s'exécuter à l'encontre de vos données ou votre réseau.

Mises à jour de sécurité & Patches

LabStats utilise un fournisseur de plateforme en tant que service (PAAS) pour héberger le Portail LabStats, et ainsi, les mises à jour de sécurité et les patches sont immédiatement installés par Microsoft au fur et à mesure de leur sortie pour les systèmes d'exploitation, les serveurs et autres logiciels de soutien. Le niveau de réactivité à ces mises à jour et les patches sont sans égal et fournissent la meilleure prévention contre des programmes malveillants et un accès non-autorisé.

Surveillance

L'infrastructure cloud sur laquelle LabStats fonctionne est surveillée physiquement, en continu, par les employés et contractants de Microsoft et virtuellement par les employés et contractants de Microsoft et les ingénieurs de LabStats.

Violation

Aucune violation de quelque nature que ce soit n'a eu lieu dans le passé et LabStats notifiera les structures en cas de violations réelles ou perçues dans le futur.

Conformité

LabStats s'efforce d'atteindre et de maintenir la conformité avec toutes les directives et standards applicables, y compris la loi relative aux droits éducatifs de la famille et la vie privée (FERPA), la loi relative aux américains handicapés (ADA) et la section 508 de la loi sur la réhabilitation. Un modèle d'auto-évaluation de l'accessibilité du produit (VPAT) est disponible sur demande.

*Ce document est fourni exclusivement à titre informatif et ne constitue pas une garantie ou un contrat entre aucune partie. Ces informations peuvent être modifiées.