Connectivité pour les systèmes d'infrastructure Dell

Table des matières

Table des matières (suite)

Introduction

1. En quoi consiste la plate-forme technologique secure connect gateway ?

La technologie secure connect gateway 5.x est le logiciel de connectivité Dell Technologies Services de nouvelle génération.

Il s'agit d'une **solution de connectivité unique permettant de gérer l'ensemble de votre portefeuille de produits d'infrastructure Dell**, à savoir les solutions de serveurs, de gestion de réseau, de stockage des données, de protection des données et d'infrastructure convergée/hyperconvergée (CI/HCI). Elle remplace les anciens logiciels SupportAssist Enterprise et Secure Remote Services dont les fonctionnalités sont intégrées à cette technologie.

Nous proposons des **options de déploiement flexibles qui peuvent être installées et mises à niveau par le client**. Avec une option de passerelle (fournie sous forme d'appliance virtuelle, d'application autonome ou d'édition Container), de connexion directe et de plug-in, vous pouvez choisir la solution qui convient le mieux à votre environnement.

Notre technologie, **également connue sous le nom de logiciel de surveillance et de support informatique à distance**, offre les avantages suivants :

- Aperçu des problèmes les plus critiques
- Résolution accélérée des problèmes grâce à un accès distant et à une communication bidirectionnelle sécurisée entre Dell Technologies et l'environnement du client
- Attention continue portée à la sécurité avec le logiciel Policy Manager doté de fonctions avancées d'audit et de contrôle, le protocole MQTT (le plus performant de sa catégorie) et de nouveaux processus de développement
- Amélioration des performances et de l'évolutivité avec la passerelle qui gère encore plus d'actions et de données de télémétrie dans votre environnement d'entreprise Dell
- Interface utilisateur Web améliorée pour notre tableau de bord de gestion de la connectivité sur site

Une fois que vous avez acheté un produit d'infrastructure Dell et qu'il est couvert par un contrat de services de support, par exemple n'importe quel niveau de service ProSupport Infrastructure Suite, vous pouvez installer ce logiciel de connectivité gratuitement. Aucune licence n'est requise.

Dès lors que notre logiciel surveille les systèmes, vous profitez de l'intégration unique d'une IA plus intelligente, d'un support automatisé et d'une analytique en temps réel.

2. Existe-t-il d'autres méthodes de connexion en dehors de l'option de passerelle ?

Oui. La technologie secure connect gateway a également été implémentée sous forme de connexion directe (sur certains produits matériels Dell) et de plug-in.

Certains produits Dell peuvent se connecter directement au back-end Dell Technologies. Ils conviennent aux clients qui ne souhaitent pas installer un logiciel distinct. Reportez-vous à la documentation relative à votre produit. *Voir la question 12 pour plus de détails.*

Les clients qui utilisent un datacenter PowerEdge avec OpenManage peuvent désormais se connecter à l'aide de notre plug-in Services pour OpenManage Enterprise afin de bénéficier de fonctions d'alerte, d'expédition automatique et de collecte.

Découvrez la technologie : rendez-vous sur Dell.com pour écouter l'avis de nos experts et accéder à des ressources techniques

Infographie avec liens utiles : Premiers pas avec la connectivité dans le datacenter

3. Les anciens logiciels SupportAssist Enterprise et Secure Remote Services ont-ils été supprimés ?

Les **éditions Virtual et Docker de Secure Remote Services v3.x** ont été entièrement supprimées le 31 janvier 2024. Le support intelligent et automatisé pour les systèmes Dell de stockage, de gestion de réseau et d'infrastructure CI/HCI pris en charge a été arrêté.

- Remarque : Les **produits Dell PowerStore et Unity qui utilisent une connexion directe** verront leur technologie supprimée le 31 décembre 2024. Pour éviter toute interruption de service, une mise à jour de l'environnement d'exploitation sera disponible avant la fin de durée de vie.

SupportAssist Enterprise versions 4.x et 2.x a été supprimé le 31 juillet 2022. Le support intelligent et automatisé pour les solutions de serveurs, de stockage, de gestion de réseau et/ou d'infrastructure CI/HCI Dell a été arrêté.

4. Ce logiciel peut-il être installé et mis à niveau par le client ?

Oui. Vous pouvez télécharger et installer notre technologie de connectivité sans l'assistance de Dell Technologies.

Rendez-vous sur le site de support Dell pour accéder aux ressources relatives à la passerelle et au plug-in.

- **Conseil :** explorez notre démo technique interactive (en anglais uniquement) pour un aperçu de l'installation, de l'enregistrement et de l'utilisation du logiciel Policy Manager et des éditions de la passerelle.

5. Ai-je besoin d'une licence ?

Aucune licence logicielle n'est requise. Toutefois, pour télécharger et enregistrer votre logiciel, vous devez être authentifié auprès du support Dell.com.

Caractéristiques et valeur ajoutée de la technologie

6. Comment l'utilisation d'un logiciel de connectivité optimise-t-elle l'expérience de support Dell ?

Les entreprises utilisent principalement nos outils de connectivité pour réduire les interruptions de service dans leur environnement, simplifier la surveillance des problèmes critiques, mais aussi identifier et résoudre des problèmes de moindre envergure avant qu'ils ne deviennent plus importants et coûteux.

La mise en place de la connectivité améliore l'expérience de support pour les produits d'infrastructure Dell couverts par des services de support, par exemple n'importe quel niveau de service ProSupport Infrastructure Suite. Une fois que notre technologie secure connect gateway (implémentée sous forme d'option de passerelle, de connexion directe ou de plug-in) surveille ces systèmes dans votre environnement, nous vous assurons un support proactif, préventif et, dans certains cas, prédictif.

Les données sont à la base de notre technologie de connectivité. **Nous tirons parti des informations sur l'état des systèmes collectées dans les environnements des clients. Nous les corrélons ensuite avec des années de données techniques et d'incidents** recueillies par nos équipes de terrain et de support technique, ainsi que par les fabricants de composants. Grâce à des **modèles d'IA sophistiqués, dont l'apprentissage automatique**, notre technologie de connectivité peut trouver et appliquer des modèles aux données de télémétrie et d'événements afin de détecter avec précision les problèmes pertinents sur lesquels agir.

Notre technologie identifie les problèmes matériels et logiciels, **crée un dossier d'incident et nous contacte pour que nous commencions à résoudre le problème avant qu'il ne devienne coûteux.** Selon le type de problème, l'alerte peut également **déclencher l'expédition automatique de pièces**, ce qui accélère la réception des pièces matérielles.

Autre fonctionnalité intéressante : le **support à distance** inclus dans la plupart de nos produits de stockage, de protection des données et d'infrastructure convergée/hyperconvergée (CI/HCI). Dans ce scénario, lorsqu'un dossier d'incident est ouvert auprès de Dell et que le problème peut être résolu à distance, la technologie assure une communication bidirectionnelle sécurisée pour permettre aux agents autorisés du support technique d'accéder à distance aux appareils gérés afin de diagnostiquer et de résoudre le problème.

De plus, grâce à l'envoi des données de télémétrie à Dell, les **données historiques de votre système contribuent à réduire le délai de résolution** lorsque l'équipe de support Dell intervient. Ainsi, quand une alerte est envoyée à Dell, un technicien du support peut se connecter à l'appareil (selon les politiques définies par le client), déterminer les mesures à prendre et fournir un plan d'action au client. Il est par exemple possible de remplacer des pièces avant même qu'elles ne tombent en panne, ce qui réduit les risques d'interruption de service.

Les **mises à niveau à distance** constituent un autre avantage des fonctionnalités de support à distance. C'est un excellent exemple de la façon dont nous utilisons notre connexion sécurisée. Le code de mise à niveau ou les correctifs de sécurité de nombreux produits peuvent être envoyés directement au client pour qu'il les applique à sa convenance. Nos équipes de gestion des changements à distance peuvent aussi planifier et exécuter la mise à niveau de A à Z sans être présentes sur site.

Écoutez l’avis de nos experts :

- Écoutez le podcast (en anglais uniquement) : Maximizing datacenter uptime with intelligent support
- Écoutez le podcast (en anglais uniquement) : Maximize PowerEdge uptime with proactive, predictive support

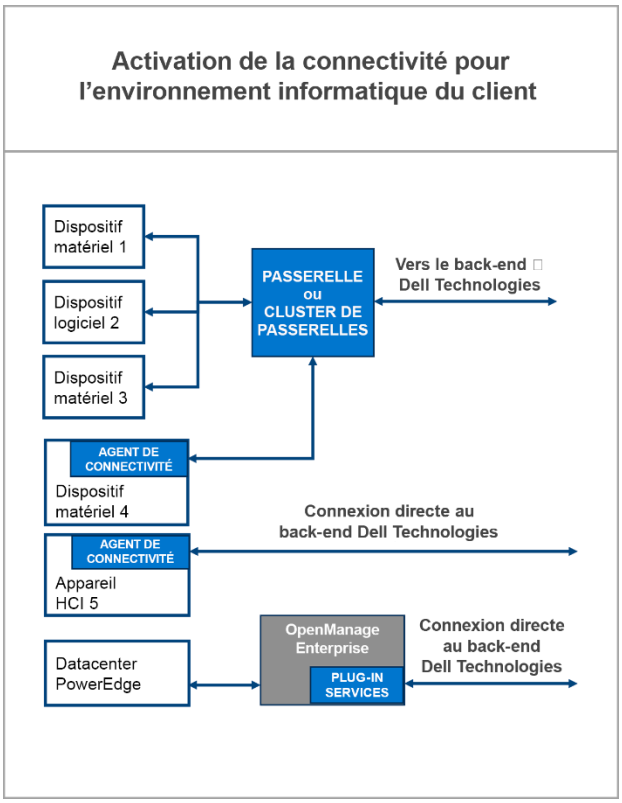
Regardez de courtes vidéos (en anglais uniquement) **:**

- Connectivity features and benefits
- Security architecture and features

Options de déploiement de la technologie

7. Quels sont les différents modes de déploiement et de configuration du logiciel de connectivité dans votre environnement ?

Grâce à nos options d'installation flexibles, vous pouvez choisir le mode qui convient le mieux à votre environnement : option de passerelle, option de connexion directe ou option de plug-in. Toutes ces options peuvent être installées et mises à niveau par le client.



L'**option de passerelle** secure connect gateway vous permet de connecter vos systèmes Dell à la passerelle pour communiquer avec Dell Technologies Services. Cette option simplifie la configuration de votre pare-feu/réseau, la passerelle étant le seul élément qui établit des connexions sortantes via Internet.

Pour l'option de passerelle, Dell propose une **édition Virtual** à l'intention des environnements VMware et Hyper-V, à laquelle s'ajoutent des **éditions Container** destinées aux environnements Docker, Podman et Kubernetes. Pour les environnements de serveurs de plus petite taille, une **édition Application** avec des versions Windows/Linux est également disponible. *Voir les questions 8 à 11.*

Les clients à la recherche de haute disponibilité et de basculement pour leurs systèmes peuvent configurer plusieurs passerelles ou un cluster afin d'assurer la redondance en cas d'indisponibilité d'une passerelle.

L'**option de connexion directe** (via l'intégration de notre technologie de connectivité dans l'environnement d'exploitation du produit Dell) s'adresse aux petits clients et aux clients non traditionnels qui ne souhaitent pas installer un logiciel supplémentaire. *Voir la question 12 pour plus d'informations.*

Enfin, nous proposons le **plug-in Services pour OpenManage Enterprise**. Destiné aux environnements axés sur le calcul, il fournit une connexion directe unique et sécurisée pour votre parc de serveurs PowerEdge. *Voir les questions 13 et 23 à 25 pour en savoir plus.*

Infographie avec liens utiles : Premiers pas avec la connectivité dans le datacenter

7 (suite). Quels sont les différents modes de déploiement et de configuration du logiciel de connectivité dans votre environnement ?

Utilisez le tableau ci-dessous pour identifier l'option la mieux adaptée à votre environnement. Vous devez consulter la matrice de support produit pour secure connect gateway ou la page de support du produit matériel sur Dell.com/Support. La version Application convient mieux aux petits clients ne disposant pas d'un environnement virtualisé et utilisant le matériel et les logiciels Dell pris en charge.

Connectez-vous pour surveiller tous les appareils depuis une même interface

Solutions intégrées	Matériel et logiciels pris en charge
Secure Connect Gateway 5.x – Virtual Appliance Edition *Pour VMware et Microsoft Hyper-V* *Packages de conteneurs : Docker, Podman, Kubernetes*	Toute la gamme de produits Dell : stockage des données, serveurs, gestion de réseau, CI/HCI et protection des données
Secure Connect Gateway 5.x – Application Edition *Administration de Windows Enterprise sur les serveurs* *Administration de Linux sur les serveurs*	PowerEdge, iDRAC, PowerSwitch, Webscale, PeerStorage, EqualLogic, Compellent, Fluid File System (FluidFS), PowerVault
Plug-in Services pour OpenManage Enterprise *Pour votre environnement OpenManage Enterprise*	Serveurs PowerEdge

Connexion directe pour certains produits matériels Dell

- Intégration de la connectivité dans l'environnement d'exploitation du produit Dell. Consultez la documentation de support du produit Dell pour connaître les modèles et versions spécifiques dotés de fonctions de connexion directe.
- Idéale pour le déploiement hétérogène de plusieurs produits matériels Dell.
- Connexion directe à Dell Technologies ou via le serveur secure connect gateway

Infographie avec liens utiles : Premiers pas avec la connectivité dans le datacenter

8. Quel est le logiciel de passerelle recommandé pour mon environnement et quelle est la configuration minimale requise ?

<table>
<tr><th colspan="2">Logiciel de passerelle</th></tr>
<tr>
<td>Secure Connect Gateway - Virtual Edition

Il existe des versions pour :
• Environnements VMware/Microsoft Hyper-V
• Packages de conteneurs : Docker, Podman, Kubernetes

Téléchargez la documentation et toutes les ressources disponibles depuis le site Dell.com/Support.</td>
<td>Secure Connect Gateway - Application Edition

Il existe des versions pour :
• Serveur d’administration Windows (surveille à la fois les appareils Windows et Linux)
• Serveur d’administration Linux (surveille les appareils Linux)

Téléchargez la documentation et toutes les ressources disponibles depuis le site Dell.com/Support.</td>
</tr>
<tr><td colspan="2">Consultez la démo technique interactive pour des conseils techniques sur l’installation, l’enregistrement et l’utilisation.</td></tr>
<tr><td colspan="2">Vérifiez la configuration minimale requise pour l’installation et l’utilisation du logiciel secure connect gateway</td></tr>
</table>

Conseils pour les nouveaux utilisateurs lors de la mise en route :

• Les nouveaux utilisateurs doivent tout d’abord créer un compte professionnel d’entreprise sur Dell.com/Support. Vous serez invité à vous connecter et à effectuer cette étape sur la page de téléchargement de secure connect gateway.

• Lorsque vous avez terminé, connectez-vous avec les informations d’identification de votre compte sur la page du support produit de secure connect gateway sur Dell.com/Support.

• Veillez à indiquer l’emplacement du site pour l’installation du logiciel. Cela nous permet de fournir une meilleure expérience de support.

• Choisissez l’édition appropriée pour votre environnement. Au cours de cette étape, vous devez créer la clé d’accès d’authentification.

Remarque : *Si vous vous connectez pour la première fois, la préparation du site est l’opération qui vous prendra le plus de temps. De plusieurs jours à plusieurs mois, selon la complexité de votre réseau et de vos politiques de sécurité. Vos équipes de sécurité et de gestion du réseau peuvent demander une revue du produit avant son implémentation.* Consultez notre livre blanc sur la sécurité.

Découvrez la technologie : rendez-vous sur Dell.com pour écouter l'avis de nos experts et accéder à des ressources techniques.

Besoin d'aide ? Interrogez nos experts sur le forum consacré à Secure Connect Gateway

9. Dois-je enregistrer mon appareil équipé de secure connect gateway auprès de Dell Technologies ?

Oui. Pour utiliser secure connect gateway et bénéficier d'une sécurité optimale, vous devez vous enregistrer auprès de Dell Technologies.

> **Conseil :** découvrez comment créer un compte professionnel d'entreprise. Une coche noire en regard de votre nom sur Dell.com/Support indique que vous êtes correctement authentifié.

À l'aide de votre compte professionnel d'entreprise, connectez-vous sur la page de téléchargement, créez une clé d'accès et un code PIN, puis utilisez ces derniers pour activer secure connect gateway.

Les clients qui ne possèdent pas de compte professionnel seront invités à fournir des informations supplémentaires sur leur organisation et leurs produits. Ils pourront poursuivre une fois le processus de vérification terminé.

10. Quelle technologie de passerelle dispose de fonctionnalités de support à distance ? Par ailleurs, quels produits possèdent des fonctions d'accès distant gérées par secure connect gateway ?

Les fonctionnalités de support à distance sont uniquement disponibles dans les éditions Virtual et Container de secure connect gateway. Elles ***ne sont pas disponibles dans l'édition Application***.

Les produits de stockage des données, de protection des données et d'infrastructure convergée/-hyperconvergée (CI/HCI) disposent de fonctions d'accès distant. Les produits PowerEdge et PowerSwitch peuvent également être configurés pour le support à distance dans l'interface utilisateur de gestion de la passerelle sur site, via le volet Présentation de l'appareil.

Les agents autorisés du support technique utilisent une authentification à deux facteurs obligatoire pour accéder à distance aux appareils gérés à des fins de dépannage et de résolution des problèmes. Toutes les sessions à distance font l'objet d'un audit, dont les détails sont accessibles à partir de la console de gestion de la passerelle sur site de secure connect gateway, dans la section Audit.

Pour un meilleur contrôle et des fonctions d'audit avancées, les clients peuvent mettre en place un serveur de gestion des règles permettant de bloquer ou d'autoriser toutes les sessions d'accès distant.

11. En quoi consiste le logiciel Policy Manager et quelle est son utilité pour l'option de passerelle ?

Policy Manager pour secure connect gateway est un logiciel externe distinct et complémentaire qui peut être installé pour des fonctions avancées d'audit et de contrôle à distance.

Policy Manager permet de définir des règles de support à distance, de transfert de fichiers et/ou d'actions à distance pour les produits prenant en charge une ou plusieurs de ces fonctions d'accès distant.

Remarque : *Policy Manager peut uniquement être utilisé avec les éditions Virtual et Container de la passerelle. Il n'est pas disponible pour l'édition Application.*

> **Conseils :** consultez le module sur la gestion des règles dans la démo interactive. Regardez les didacticiels vidéo techniques consacrés à l'édition Virtual Appliance.

12. Quels sont les produits compatibles avec la connexion directe ? Puis-je également utiliser la connexion directe avec une passerelle ?

Dans certains cas, notre technologie de connectivité est intégrée à l'environnement d'exploitation du produit Dell et permet une connexion directe à notre back-end des services. C'est ce que l'on entend par « connexion directe ».

Vous serez invité à activer les services de connectivité lors de la configuration de vos produits matériels et logiciels Dell.

Cependant, vous pourrez à tout moment basculer entre une connexion directe et une connexion via une passerelle sur votre produit Dell. Les politiques de sécurité et de gestion de réseau de votre entreprise influenceront vos décisions en matière de configuration.

Produits d'infrastructure Dell compatibles avec la connexion directe *Vérifiez toujours la liste la plus récente des produits pris en charge sur Dell.com/Support*
AppSync | APEX AIOps Infrastructure Observability Collector | Logiciel CMS - VxBlock
Data Backup/Avamar | Data Domain | Data Domain Management Console | Edge Orchestrator
Elastic Cloud Storage | Metro Node Appliances | ObjectScale
Famille PowerFlex - Appliance, rack, logiciels
PowerProtect - Data Manager, appliance Data Manager, appliance scale-out
PowerScale | PowerStore | PowerVault | Série S5000 | SRM | Streaming Data | Unity | VxRail
Consultez la documentation de support de votre produit pour connaître les modèles et versions spécifiques dotés de fonctions de connexion directe.

Remarque : *Les fonctionnalités logicielles de SupportAssist, SupportAssist Enterprise et Secure Remote Services font désormais partie de notre plate-forme logicielle de connectivité de nouvelle génération. Les références à ces logiciels dans l'interface utilisateur de votre produit seront progressivement mises à jour en conséquence.*

13. En quoi consiste le plug-in Services pour OpenManage Enterprise ?

La technologie secure connect gateway a également été implémentée sous forme de plug-in. Les clients qui utilisent un datacenter PowerEdge avec OpenManage peuvent désormais se connecter à l'aide de notre plug-in Services pour OpenManage Enterprise afin de bénéficier de fonctions d'alerte, d'expédition automatique et de collecte.

Ressources :

- En savoir plus sur le plug-in et accéder à des ressources techniques
- Pour obtenir la liste des produits pris en charge, consultez la matrice de support produit sur la page de support produit d'OpenManage Enterprise Services.

Écoutez l'avis de nos experts :

- **Regardez une courte vidéo** (en anglais uniquement) **:** Services plugin for OpenManage Enterprise
- **Écoutez le podcast** (en anglais uniquement) **:** Maximize PowerEdge uptime with proactive, predictive support
- **Consultez :** Livre blanc sur la sécurité

14. Comment obtenir de l'aide pour déployer le logiciel de connectivité ?

De nombreux clients téléchargent et installent notre technologie de connectivité sans l'assistance de Dell Technologies. Rendez-vous sur notre page Web pour accéder à toutes les ressources disponibles.

Conseil : vous pouvez lancer et explorer notre démo technique interactive

- *Découvrez comment installer, enregistrer et utiliser les éditions de la passerelle et Policy Manager*

Si vous avez besoin d'assistance, l'activation et la configuration de secure connect gateway sont incluses dans les services de l'offre ProDeploy Infrastructure Suite.

Les clients bénéficiant de la couverture ProSupport Plus se voient attribuer un Service Account Manager (SAM) qui pourra répondre à leurs questions sur l'installation et l'enregistrement.

Sinon, ils devront contacter le support Dell Technologies pour obtenir de l'aide.

15. Comment contacter le support en cas de problème ?

Si vous rencontrez des problèmes avec le support en ligne sur Dell.com ou avec secure connect gateway, rendez-vous sur notre page de support administratif accessible ici pour obtenir de l'aide. Sélectionnez la catégorie qui se rapproche le plus de votre problème et fournissez les informations demandées. Si vous avez besoin d'une assistance immédiate pour un problème de support technique, contactez-nous ici. Veuillez contacter votre Service Account Manager (le cas échéant).

Sécurité

16. J’aimerais en savoir plus sur ce logiciel dans l’environnement du client et sur la connexion à Dell. Comment est-elle sécurisée ?

La connexion entre votre environnement et Dell est sécurisée par un tunnel TLS mutuel et une chaîne de certificats. Dans ce type de configuration, vos systèmes se connectent à notre logiciel dans votre environnement et ces connexions ne nécessitent que des changements de ports/réseau internes. Le logiciel est le seul élément qui établit une connexion sortante via Internet vers Dell. Il agit comme un point d’agrégation pour les événements et les données de télémétrie de tous vos systèmes connectés. Ce sont les seules informations sur l’état du système qui sont envoyées.

Toutes les données de télémétrie des systèmes sont transportées via le protocole HTTPS TLS 1.3. Nous proposons également des fonctionnalités de support à distance via le tunnel sécurisé pour accéder à votre système et le dépanner, ce qui accélère la résolution des problèmes et évite les interruptions de service.

Pour en savoir plus, consultez notre livre blanc sur la sécurité.

17. Comment se déroule le support à distance ? Quels collaborateurs Dell peuvent accéder au système via une session de support à distance ?

Les ingénieurs du support technique Dell créent des sessions de support à distance depuis un portail afin d’accéder à vos systèmes pour les activités de dépannage et de mise à niveau. L’accès à ce portail requiert une authentification multifacteur. Les collaborateurs Dell doivent suivre une formation rigoureuse et obtenir l’autorisation de la direction pour accéder au portail. Nous utilisons le protocole MQTT, solution très répandue pour les systèmes d’entreprise connectés, en tant qu’agent de support à distance.

18. Compte tenu de l’importance accordée à la sécurité, les informations sur l’état du système, les événements et les données de télémétrie font-ils l’objet d’un audit ? Quel est le rôle de Policy Manager ?

Nous auditons toutes les transactions et ces informations sont consultables dans l’interface utilisateur du logiciel. Les sessions de support à distance, les événements et les transferts de données de télémétrie sont tous disponibles pour consultation.

Si les clients utilisent des politiques de sécurité plus strictes ou si des auditeurs tiers ont besoin de stocker ces informations pendant une longue période, nous recommandons d’installer notre logiciel Policy Manager. Policy Manager fonctionne avec secure connect gateway pour fournir des fonctions avancées d’audit et de contrôle du support à distance. *Voir aussi la question 11.*

19. Où puis-je trouver de plus amples informations sur l'architecture de sécurité de la technologie de connectivité ?

Téléchargez le livre blanc sur la sécurité et découvrez comment la technologie secure connect gateway intègre la protection des données et la prévention des menaces pour fournir une expérience de support automatisée et sécurisée.

Ce document traite des sujets suivants :

- **Collecte sécurisée des données sur site :** découvrez comment secure connect gateway agit en tant que courtier de communications sécurisé, permet aux clients de contrôler les exigences en matière d'autorisation, utilise des protocoles d'authentification à deux facteurs et bien plus encore.
- **Communication et transport sécurisés des données :** découvrez comment secure connect gateway utilise le chiffrement et l'authentification bilatérale afin de créer un tunnel TLS (Transport Layer Security) pour ses fonctions d'interrogation des pulsations, de notification à distance et d'accès distant.
- **Stockage, utilisation et traitement sécurisés des données :** découvrez-en plus sur les mesures quotidiennes mises en œuvre pour protéger vos données, notamment la sécurité physique, la gestion des risques au niveau de la chaîne logistique et les processus de développement sécurisé.

Écoutez l'avis de nos experts :

- **Écoutez le podcast** (en anglais uniquement) **:** Maximizing datacenter uptime with intelligent support
- **Consultez :** Livre blanc sur la sécurité

Regardez de courtes vidéos (en anglais uniquement) **:**

- Security architecture and features
- Security configuration for large and small scale environments
- Security features for financial sector

Ou regardez le webinaire (en anglais uniquement) **:** écoutez nos experts lors de l'événement organisé par la communauté Spiceworks. Ils abordent les sujets suivants :

- Comment secure connect gateway intègre la confidentialité, la protection des données et la prévention des menaces
- Comment déployer la connectivité de manière flexible dans des environnements de petite taille, de grande taille et non traditionnels
- Comment le support automatisé prévient et atténue les problèmes liés aux systèmes connectés

Scénarios de configuration

20. Quels sont les facteurs à prendre en compte pour le déploiement et la configuration de la technologie de connectivité en fonction des besoins de votre entreprise ?

Les premiers facteurs à prendre en considération sont les **types de produits, à savoir calcul, stockage, protection des données, infrastructure convergée/hyperconvergée (CI/HCI),** que vous allez configurer pour la connectivité, ainsi que **votre environnement actuel**. Par exemple :

- Vos datacenters sont-ils reliés en réseau ?
- Gérez-vous les systèmes de calcul et de stockage (y compris les produits de protection des données et CI/HCI) *séparément ou ensemble* ?

Vous devez également tenir compte des **politiques de sécurité et de gestion de réseau** de l'entreprise. Il convient en outre de savoir **si vos équipes souhaitent gérer tous les produits ensemble ou si elles préfèrent les segmenter par géolocalisation ou type de produit.**

Vous devez essentiellement vous demander comment les éléments sont connectés entre eux, comment les équipes travaillent ensemble et comment réduire la complexité du réseau. Vous pourrez ainsi concevoir l'architecture la plus efficace en fonction des différentes options de déploiement.

Lisez et partagez notre présentation des facteurs à prendre en considération pour la configuration de la connectivité. Elle aborde les sujets suivants :

1. Quelle est la configuration recommandée pour une grande entreprise soucieuse de la sécurité ?
2. Quelles sont les options de configuration et de déploiement pour les petites et moyennes organisations ?
3. Que se passe-t-il pour les grandes et moyennes entreprises dont l'environnement est axé sur le calcul ? Quel outil doivent-elles choisir d'utiliser ?
4. Que se passe-t-il si je possède entre 1 et 50 serveurs PowerEdge, mais pas d'environnement virtualisé ? Quelles sont mes options de passerelle ?
5. Que se passe-t-il si je dispose de produits Dell avec connexion directe ? Quels sont les principaux cas d'utilisation ?
6. Quelle est la meilleure configuration pour mon entreprise ?

Services de support

21. Quelle valeur ajoutée la connectivité apporte-t-elle au contrat de services de support de mes produits d'infrastructure Dell ?

En résumé, vous pouvez tirer davantage parti de vos contrats de support actifs sur les systèmes Dell en déployant notre logiciel de connectivité dans votre environnement et en connectant vos appareils Dell pour qu'ils soient surveillés par ce logiciel. Ce logiciel est gratuit. Aucune licence n'est nécessaire. Nous prenons en charge plus de 90 produits d'infrastructure Dell, aussi bien matériels que logiciels. Vous profiterez de l'intégration unique d'une IA plus intelligente, d'un support automatisé et d'une analytique en temps réel.

Les clients ayant souscrit des services ProSupport Infrastructure Suite bénéficient d'avantages à tous les niveaux.

- En savoir plus : Couverture ProSupport et ProSupport Plus pour les systèmes d'infrastructure Dell
    - En savoir plus : Lifecycle Extension with ProSupport ou ProSupport Plus
- Remarque : Les systèmes Dell couverts par un contrat Basic Hardware Support (jour ouvré suivant) profitent également de nos fonctions proactives et automatisées de détection des problèmes, de création de dossiers d'incident et de notification lorsqu'ils sont surveillés par notre logiciel de connectivité. Lorsqu'un problème est détecté, les clients détenteurs d'un contrat de support de base reçoivent un e-mail contenant le numéro de dossier et sont invités à contacter le support Dell dans les meilleurs délais pour confirmer qu'ils souhaitent bénéficier de l'assistance de Dell pour le dépannage et la résolution du problème.

Découvrez également nos services de support spécialisés pour l'infrastructure

22. Qu'advient-il des fonctions de support automatisées une fois le contrat de services de support, par exemple avec ProSupport Infrastructure Suite, arrivé à expiration pour mon système surveillé ?

Si votre contrat de service pour n'importe quel niveau de l'offre ProSupport Infrastructure Suite arrive à expiration, la fonction de création automatique de dossiers d'incident sera désactivée. La technologie secure connect gateway déployée en tant que passerelle, connexion directe ou plug-in continuera toutefois à exécuter des collectes automatisées d'informations sur l'état du système. Si vous mettez à niveau ou prolongez votre contrat sur un système (étiquette de service), la création automatique de dossiers d'incident sera automatiquement réactivée sur ce système.

Connectivité pour PowerEdge

23. Quelles sont les meilleures façons de déployer et de configurer ce logiciel de connectivité pour les serveurs ? Comment choisir l'outil à utiliser ?

En résumé, le plug-in Services de la solution OpenManage Enterprise convient aux clients dont les environnements sont axés sur le calcul, tandis que la solution de passerelle est idéale pour gérer divers produits d'infrastructure Dell.

Les deux solutions incluent nos fonctions d'alerte, de création automatique de dossiers d'incident, d'expédition automatique et de collecte des données de télémétrie pour les serveurs PowerEdge couverts par un contrat de support.

Le choix dépendra du type d'environnements, de la façon dont ils sont connectés entre eux, des types d'appareils surveillés et de vos préférences.

Si vous avez installé OpenManage Enterprise ou envisagez de le faire, le plug-in Services est fait pour vous. OpenManage Enterprise est la solution d'infrastructure de Dell qui permet de gérer le cycle de vie de milliers de serveurs PowerEdge depuis une même console.

- Si vous êtes novice dans ce domaine, il vous suffit d'installer OpenManage Enterprise dans votre environnement, d'intégrer vos serveurs, puis d'installer notre plug-in Services (en vous assurant que votre pare-feu est correctement configuré) pour que le plug-in commence à envoyer des alertes et des données de télémétrie à Dell.

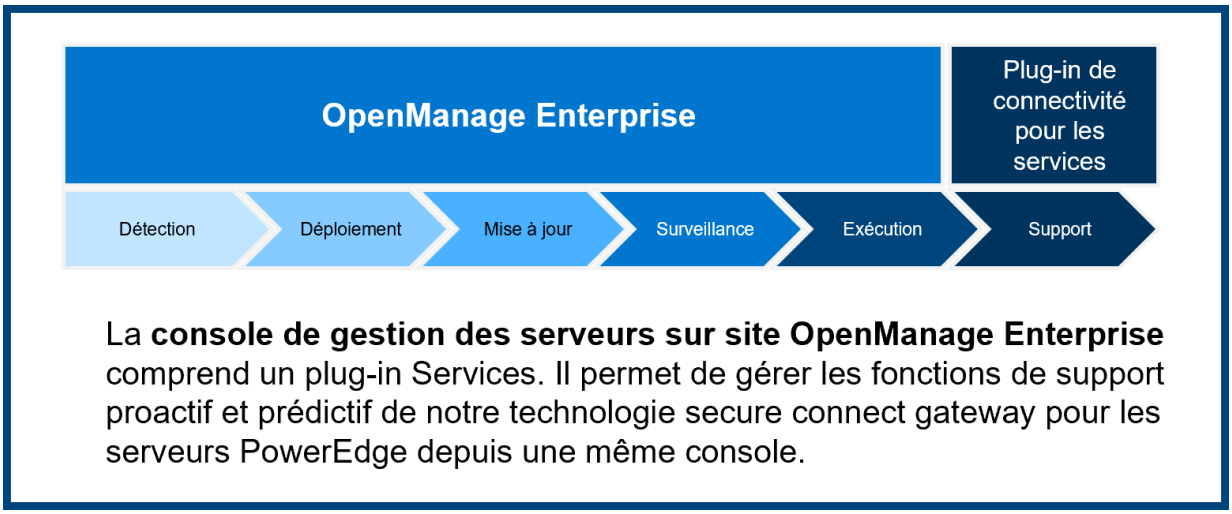
Les clients qui utilisent différents produits d'infrastructure Dell, comme Powerstore, PowerMax, PowerScale, Data Domain et VxRail, parallèlement à PowerEdge ont davantage intérêt à installer notre solution secure connect gateway afin de gérer ces systèmes depuis une même interface utilisateur.

Écoutez l'avis de nos experts :

- **Écoutez le podcast** (en anglais uniquement) **:** Maximize PowerEdge uptime with proactive, predictive support
  - En quoi consiste la connexion de systèmes PowerEdge via la solution OpenManage Enterprise et en quoi diffère-t-elle de la connexion via une solution de passerelle ?
  - Comment se connecter aux appareils PowerEdge eux-mêmes ?
  - Comment augmenter facilement le nombre de serveurs connectés au fil du temps ?
  - Autres scénarios de configuration : exécution en parallèle de l'option de plug-in et de passerelle

24. Comment la connectivité pour les services complète-t-elle la surveillance du cycle de vie de la gestion du datacenter par OpenManage Enterprise ?

OpenManage Enterprise est une console de gestion de systèmes simple à utiliser de type « un à plusieurs ». Elle permet de gérer le cycle de vie complet des serveurs et des boîtiers PowerEdge de façon économique depuis une même console. Le diagramme ci-dessous explique comment le plug-in de connectivité pour OpenManage Enterprise complète l'expérience OpenManage Enterprise pour le datacenter. Cette fonctionnalité est actuellement disponible via le plug-in Services pour OpenManage Enterprise. En savoir plus et trouver des ressources.



25. Quels systèmes sont pris en charge par le plug-in Services pour OpenManage Enterprise ?

Les serveurs et les boîtiers PowerEdge avec iDRAC et Chassis Management Controller (CMC), ainsi que les serveurs Linux, sont pris en charge.

Pour obtenir la liste des produits spécifiques pris en charge, rendez-vous sur le site Dell.com/Support et consultez la matrice de support sur la page de support produit d'OpenManage Enterprise Services.

Informations générales

26. Où puis-je trouver des informations sur les politiques d'alerte de secure connect gateway ? Quand des dossiers d'incident prédictifs sont-ils ouverts pour les pannes matérielles ?

La politique d'alerte de Secure Connect Gateway fournit des informations sur les alertes entraînant l'ouverture de dossiers d'incident auprès du support technique de Dell Technologies. Les clients qui utilisent secure connect gateway reçoivent uniquement des alertes relatives à la création automatique de dossiers d'incident prédictifs pour le matériel de serveur (disques durs, fonds de panier et cartes d'extension) sur les systèmes couverts par les services ProSupport Plus. Les alertes prédictives sont basées sur les collectes de données planifiées envoyées à Dell Technologies.

27. Que dois-je savoir sur les fonctions de la passerelle en matière de gestion des informations d'identification ?

Secure connect gateway offre la possibilité d'ajouter plusieurs profils et comptes d'identification. Grâce aux comptes d'identification, les administrateurs peuvent ajouter une authentification en fonction du type de produit. Les profils permettent quant à eux à plusieurs administrateurs, qui diffèrent par leur fonction ou leur zone géographique, de gérer leurs comptes spécifiques. Les produits pour lesquels des informations d'identification sont requises sont les solutions PowerEdge, iDRAC, Compellent, de gestion de réseau, PS Series, MD Series et Webscale.

Nous proposons également l'intégration d'un coffre-fort d'informations d'identification. Grâce à cette solution, les clients possédant de nombreux appareils peuvent ajouter des systèmes et stocker les informations d'identification appropriées sans compromettre la sécurité ni augmenter la charge de travail manuelle. Les API CyberArk Conjur et les produits CyberArk Credential Provider sont actuellement pris en charge. D'autres fournisseurs seront ajoutés. Consultez notre documentation de support pour obtenir la liste la plus récente.

Conseil : découvrez ces fonctionnalités dans le module *Device Management* de la démo interactive

28. Quelles sont les principales fonctionnalités du mode maintenance ?

Une « tempête d'événements » survient lorsque des alertes matérielles se produisent à la chaîne en dépassant le nombre limite prédéfini d'alertes. Dans ce scénario, secure connect gateway interrompt le traitement des alertes pour les appareils à l'origine de la tempête d'événements. Tous les autres appareils continuent à être surveillés par secure connect gateway afin d'identifier les alertes validées pouvant entraîner l'ouverture de dossiers d'incident.

En outre, les utilisateurs ont désormais la possibilité d'activer manuellement le mode maintenance sur un ou plusieurs appareils à partir du système. Cette fonctionnalité peut être utilisée pour les opérations de maintenance planifiées et déployée lorsque vous ne souhaitez pas que secure connect gateway surveille ces appareils. Une fois les activités de maintenance planifiées terminées, vous pouvez désactiver manuellement le mode maintenance pour que secure connect gateway reprenne la surveillance.

29. L'option de passerelle permet-elle de définir des préférences de notification par e-mail ?

Oui. Vous pouvez personnaliser vos préférences de notification par e-mail sous l'onglet Paramètres de l'interface utilisateur de secure connect gateway. Consultez le guide de l'utilisateur pour plus de détails.

30. Quelles sont les langues prises en charge dans le tableau de bord de gestion de la passerelle sur site ?

L'interface logicielle de secure connect gateway est disponible en anglais, allemand, portugais brésilien, français, espagnol, chinois simplifié et japonais. Toutefois, les clients peuvent choisir parmi 28 langues pour les notifications par e-mail automatiques envoyées lors d'une demande de service. Remarque : Certaines notifications par e-mail ne sont pas traduites dans la langue locale en raison des limitations du système d'exploitation.

31. Comment bien démarrer avec les API REST ?

Avec l'option de passerelle, les clients peuvent exécuter et prendre en charge leurs propres scripts personnalisés avec des API REST. Téléchargez le guide de l'utilisateur des API REST depuis notre section Documentation.

32. Comment ce logiciel de connectivité est-il utilisé avec APEX AIOps Infrastructure Observability (anciennement CloudIQ) ?

APEX AIOps Infrastructure Observability (anciennement CloudIQ) permet d'optimiser l'intégrité, la cybersécurité et la durabilité de l'infrastructure Dell de datacenter, de périphérie et multicloud en fournissant des informations et des recommandations basées sur l'IA.

- Ses principaux avantages sont les suivants : évaluation de l'intégrité et des risques de cybersécurité avec recommandations de mesures correctives ; suivi des performances et de la capacité ; détection des anomalies et prévisions ; prévision des défaillances ; suivi et prévision de la consommation énergétique et des émissions ; et surveillance des ressources de virtualisation.

Notre logiciel de connectivité sert uniquement à transmettre les données relatives au système et aux événements depuis l'environnement du client. Les données de télémétrie sont envoyées en toute sécurité au back-end Dell où elles sont analysées par les algorithmes d'IA d'APEX AIOPs Infrastructure Observability.

Fonctionnalité clé (sans rapport avec la connectivité) :

- Sur le portail Infrastructure Observability, vous pouvez également tirer parti de l'Assistant AIOps qui utilise l'IA générative pour fournir des réponses instantanées et détaillées, ainsi que des recommandations pour résoudre les problèmes liés à l'infrastructure Dell.