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 pour gérer l'ensemble de votre infrastructure Dell**, c'est-à-dire les serveurs, les réseaux, le stockage de données, la protection des données et les solutions d'infrastructure convergée et hyperconvergée (CI/HCI). Elle remplace également les logiciels existants, 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 :

- Un aperçu des problèmes les plus critiques
- Accélération de la résolution des problèmes avec un accès distant et 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
- Une expérience d'utilisation de l'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 backend Dell Technologies et sont adaptés aux clients qui ne souhaitent pas configurer des logiciels distincts. Veuillez vous référer à la documentation relative à votre produit. *Lisez les questions Q12 et Q28 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 mises hors service le 31 janvier 2024. Le support intelligent et automatisé pour le stockage, la mise en réseau et les systèmes de conteneurs intégrés (CI/HCI) pris en charge par Dell a été interrompu.

- Remarque : Pour les clients disposant de produits **Dell PowerStore et Unity qui utilisent la connexion directe**, leur technologie a été mise hors service le 31 décembre 2024. Pour éviter les interruptions de service, une mise à jour de l'environnement d'exploitation est disponible avant la fin de la durée de vie.

SupportAssist Enterprise 4.x et 2.x ont été mis hors service le 31 juillet 2022. Le support intelligent et automatisé pour le serveur, le stockage, la mise en réseau et les systèmes de conteneurs intégrés (CI/HCI) pris en charge par Dell a été interrompu.

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 configuration de la connectivité améliore l'expérience de support pour les produits d'infrastructure Dell avec une couverture de services de support, par exemple, avec n'importe quel niveau de service pour ProSupport Infrastructure Suite. Lorsque notre technologie Secure Connect Gateway, mise en œuvre en tant que passerelle, connexion directe ou plug-in, surveille ces systèmes dans votre environnement, nous vous fournissons un support proactif, préventif et, dans certains cas, prédictif.

La technologie de connectivité repose sur les données. **Nous exploitons les données d'état des systèmes provenant des environnements clients. Et nous les corrélons avec des années de données d'incidents et d'ingénierie** provenant des équipes de support technique et d'intervention, ainsi que des fabricants de composants. À l'aide de **modèles d'IA sophistiqués, y compris 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 le problème sur lequel agir.

Notre technologie identifie les problèmes matériels et logiciels, **crée un dossier et initie un contact avec nous pour commencer à résoudre un problème avant qu'il ne devienne coûteux.** En fonction du type de problème, l'alerte peut également **déclencher une expédition automatique de pièces**, ce qui signifie une réception plus rapide des pièces matérielles.

La **prise en charge à distance** de la plupart de nos produits de stockage, de protection des données, convergés et hyperconvergés (CI/HCI) est une autre fonctionnalité intéressante. Dans ce scénario, lorsqu'un dossier est ouvert de notre côté, si nous pouvons le résoudre via le support à distance, la technologie permet une communication bidirectionnelle sécurisée pour que les agents du support technique agréés puissent accéder à distance aux appareils gérés afin de diagnostiquer et de résoudre les problèmes.

En outre, en renvoyant les données de télémétrie à Dell, les **données historiques de votre système peuvent vous aider à réduire le délai de résolution** lorsque le support Dell intervient. Par exemple, lorsqu'une alerte est renvoyée à Dell, un technicien de support peut se connecter à l'appareil (en fonction des politiques définies par le client), puis confirmer les actions à entreprendre et fournir au client un plan d'action. Par exemple, les pièces peuvent être remplacées avant qu'elles ne tombent en panne, ce qui minimise le risque de temps d'arrêt.

Les **mises à niveau à distance** sont un autre avantage des fonctions de support à distance. Il s'agit d'un excellent exemple d'utilisation de notre connexion sécurisée. De nombreux produits peuvent avoir un code de mise à niveau ou des correctifs de sécurité envoyés directement au client pour qu'il puisse les appliquer à sa convenance. Nos équipes de gestion des changements à distance peuvent également planifier et exécuter la mise à niveau du début à la fin sans être 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

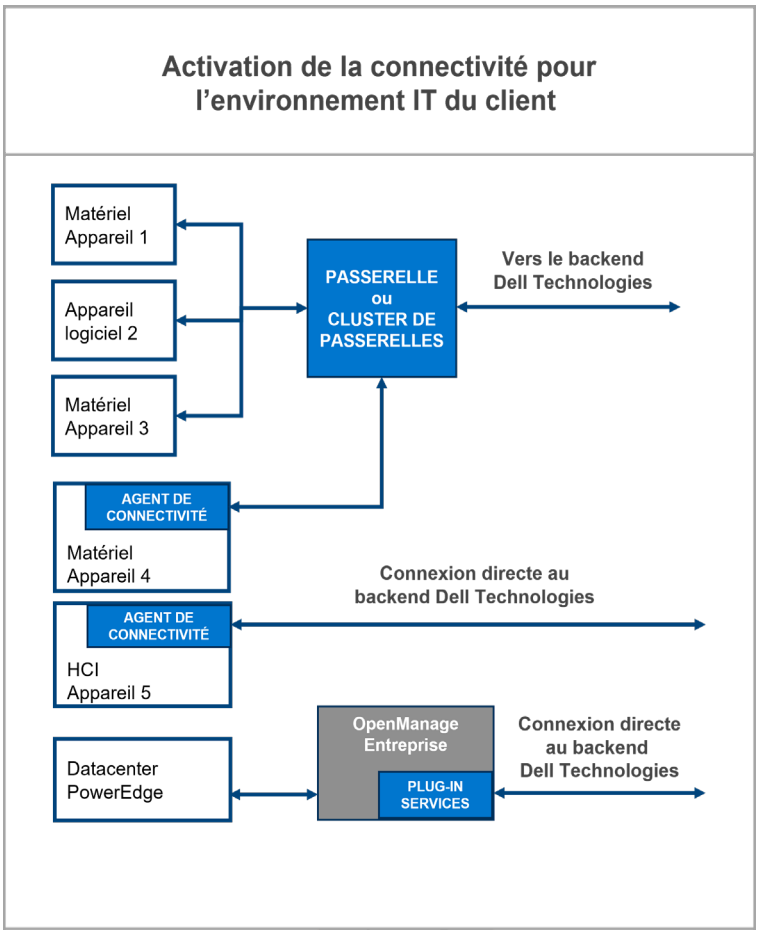
Regardez de courtes vidéos (en anglais uniquement) **:**

- 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. Elles peuvent toutes être installées et mises à niveau par le client.



L'option **Secure Connect Gateway** vous permet de connecter vos systèmes Dell à la passerelle pour communiquer avec Dell Technologies Services. Cela simplifie la configuration de votre pare-feu/réseau, de sorte que la passerelle est la seule connexion sortante sur Internet.

Pour notre option de passerelle, Dell propose une **édition Virtual** pour les environnements VMware, Microsoft Hyper-V et Linux KVM. Nous proposons également des **éditions Container** pour les environnements Docker, Podman, Kubernetes et OpenShift. Pour nos clients de serveurs plus petits, nous proposons une **édition Application** avec les versions Windows/Linux. *Voir l'article Q8-11 de la base de connaissances.*

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 de logiciels supplémentaires. *Voir les questions Q12 et Q28 pour plus de détails.*

Enfin, nous proposons le **plug-in Services pour OpenManage Enterprise**. Destiné aux clients axés sur le calcul, il fournit une connexion directe unique et sécurisée pour votre parc de serveurs PowerEdge. *Voir les questions Q13 et Q23-25 pour plus de détails.*

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 appropriée pour votre environnement. Consultez la matrice de support produit pour Secure Connect Gateway ou rendez-vous sur la page du support matériel sur Dell.com/Support. La version Application est idéale pour les petits clients qui ne disposent pas d'un environnement virtualisé et qui utilisent le matériel et les logiciels Dell pris en charge.

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

Solutions intégrées

Solutions intégrées	Matériel et logiciels pris en charge
Secure Connect Gateway 5.x – Édition Virtual Appliance *Pour les environnements VMware, Microsoft HyperV et Linux KVM* *Packages de conteneurs : Docker, Podman, Kubernetes, OpenShift*	Gamme complète de produits Dell : stockage des données, serveurs, mise en réseau, CI/HCI et protection des données
Secure Connect Gateway 5.x – Édition Application *Gestion Windows Enterprise sur les serveurs* *Gestion 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.
- 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 ?

Logiciel de passerelle	
Secure Connect Gateway - Virtual Edition Il existe des versions pour : • Environnements VMware, Microsoft HyperV et Linux KVM • Packages de conteneurs : Docker, Podman, Kubernetes, OpenShift Téléchargez la documentation et toutes les ressources disponibles depuis le site Dell.com/Support.	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.
Consultez la démo technique interactive pour des conseils techniques sur l'installation, l'enregistrement et l'utilisation.	
Vérifiez la configuration minimale requise pour l'installation et l'utilisation du logiciel secure connect gateway	

Quatre étapes à suivre pour connecter les clients

1. **Préparez le site et vérifiez le compte**

   Prévisualisez les exigences techniques et planifiez l'administrateur réseau. Avant l'étape 2, configurez un compte professionnel d'entreprise sur Dell.com/Support.

2. **Télécharger**

   Connectez-vous avec les informations d'identification de votre compte sur la page de support produit de Secure Connect Gateway sur Dell.com/Support.

   Obtenez l'édition appropriée pour l'environnement du client et créez la clé d'accès d'authentification.

3. **Installer et provisionner**

   Déployez le modèle d'appliance virtuelle ou de conteneur ou installez le logiciel applicatif. Suivez les étapes de l'inscription initiales.

4. **Connecter leurs appareils**

   Configurez et activez les communications entre les produits Dell du client et le serveur de passerelle.

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

- Les nouveaux utilisateurs doivent configurer un compte professionnel d'entreprise sur Dell.com/Support. À partir de la page de téléchargement de Secure Connect Gateway, vous serez invité à vous connecter et à effectuer cette étape.
- 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.
- Renseignez l'emplacement du site pour l'installation du logiciel. Cela nous permet d'offrir une meilleure expérience d'assistance.
- Sélectionnez la bonne édition pour votre environnement. Au cours de cette étape, vous devez créer la clé d'accès d'authentification.

Remarque : *Pour ceux qui se connectent pour la première fois, la préparation du site est l'étape la plus longue. De quelques jours à plusieurs mois, selon la complexité de votre réseau et de vos politiques de sécurité. Vos équipes de sécurité et de gestion réseau peuvent demander un examen du produit avant la mise en œuvre.* Voir notre document 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 ne possédant pas de compte professionnel devront fournir des informations supplémentaires sur leur organisation et leurs produits. Ils pourront continuer après avoir suivi le processus de vérification.

10. Quelle technologie de passerelle offre des fonctionnalités de support à distance ? Et quels produits ont des capacités 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 de données, de protection des données, convergés et hyperconvergés (CI/HCI) sont dotés de fonctionnalités d'accès distant. Les produits PowerEdge et PowerSwitch peuvent également être activés pour le support à distance dans l'interface utilisateur de gestion de passerelle sur site via Device Overview.

Les agents de support technique agréés utilisent une authentification à deux facteurs requise pour accéder à distance aux appareils gérés afin de dépanner et de résoudre les problèmes. Toutes les sessions à distance sont auditées et les détails sont accessibles à partir de la console de gestion de passerelle sur site pour Secure Connect Gateway, sous 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 de gestion des politiques dans la démonstration interactive. Regardez les vidéos techniques pour l'édition Virtual Appliance.

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

Dans certains cas, notre technologie de connectivité est intégrée dans l'environnement d'exploitation du produit Dell et permet une connexion directe à notre back-end de 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.

Toutefois, à tout moment, vous pouvez commuter votre produit Dell compatible avec la connexion directe pour qu'il se connecte via une passerelle. Les politiques de sécurité et de gestion de réseau de votre entreprise impacteront vos décisions 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 des logiciels SupportAssist, SupportAssist Enterprise et Secure Remote Services font désormais partie de notre plateforme logicielle de connectivité de nouvelle génération. Ces références logicielles dans l'interface utilisateur de votre produit seront mises à jour en conséquence au fil du temps.*

Pour plus d'informations sur l'option de connexion directe pour les serveurs, veuillez *lire la question Q28*.
Remarque : La connexion via une passerelle est impossible.

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. *Voir également la question Q27.*

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. Pour accéder à toutes les ressources, consultez notre page Web.

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 Technical Customer Success Manager 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 Dell.com ou Secure Connect Gateway, rendez-vous sur notre page Support administratif à partir de cet emplacement pour demander de l’aide. Sélectionnez la catégorie qui correspond le mieux à votre problème et remplissez les détails comme indiqué. Si vous avez besoin d’une assistance immédiate pour un problème de support technique, contactez-nous ici. Contactez votre Technical Customer Success Manager (si applicable).

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 via un tunnel TLS mutuel et une chaîne de certificat. Dans ce type de configuration, vos systèmes se connecteront à notre logiciel dans votre environnement et ces connexions ne devront être que des modifications de port interne/réseau. Le logiciel sera la seule méthode de connexion sortante vers Internet et à Dell. Il sert de point d’agrégation pour tous vos systèmes connectés pour les données d’événement et de télémétrie. Il s’agit de la seule information sur l’état du système envoyée.

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-elles 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 également la question Q11.*

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 des données sécurisés :** découvrez comment la Passerelle de connexion sécurisée utilise le chiffrement et l'authentification bilatérale pour créer un tunnel avec le protocole TLS pour l'interrogation des pulsations, les notifications à distance et les fonctions d'accès distant.
- **Traitement, utilisation et stockage des données sécurisés :** découvrez plus d'informations sur les mesures mises en œuvre quotidiennement pour protéger vos données, notamment la sécurité physique, la gestion des risques de la chaîne d'approvisionnement 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.**

En fait, vous devez réfléchir à la façon dont les éléments sont liés, dont les équipes travaillent ensemble et de réduire la complexité du réseau. Cela vous permettra de 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 une connexion directe ? Quels sont les principaux cas d'utilisation ?
6. Quelle est la meilleure configuration pour mon entreprise ?

Services de

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 :

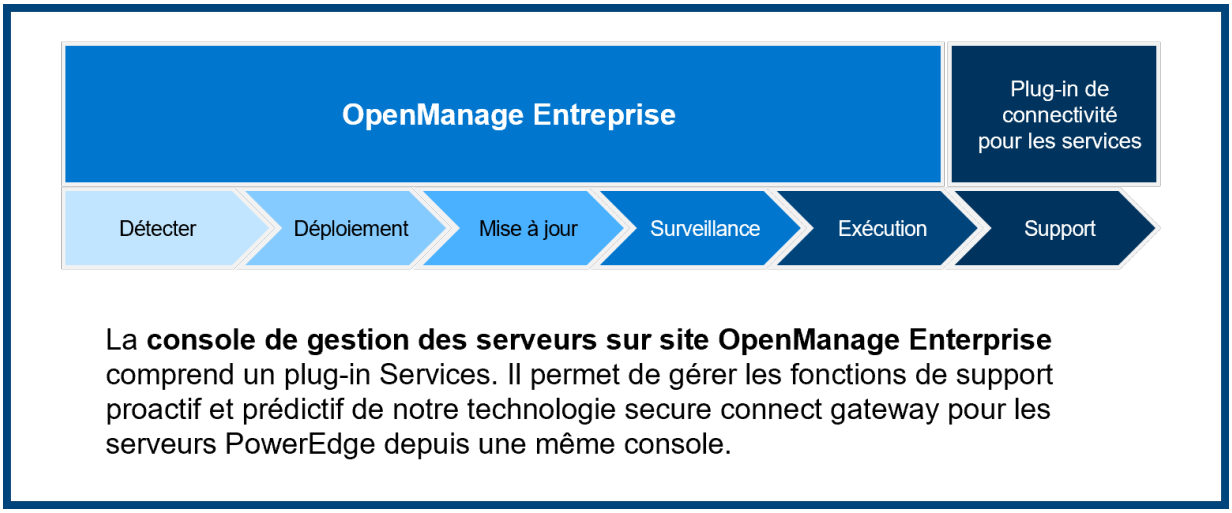
- **Écoutez le podcast** (en anglais uniquement) **:** Maximize PowerEdge uptime with proactive, predictive support
    - En quoi consiste la connexion de systèmes PowerEdge via la solution OpenManage Enterprise et en quoi diffère-t-elle de la connexion via une solution de passerelle ?
    - Comment 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

Mise à jour de l'option de connexion directe pour les serveurs

- *Lisez la question Q28* pour obtenir tous les détails, y compris les informations spécifiques aux produits et aux régions, ainsi que des conseils sur les éléments de connectivité à prendre en compte.

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 Entreprise 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 châssis 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.

26. Le logiciel de connectivité pour les services me permet-il d'effectuer des tâches de gestion du cycle de vie du datacenter pour les serveurs PowerEdge, comme OpenManage Enterprise ?

Non. Notre logiciel de connectivité pour les services ne transfère ni n'orchestre les mises à jour du BIOS et du firmware pour les appareils PowerEdge autonomes dans un datacenter. En général, les clients axés sur le calcul disposant d'environnements de serveurs autonomes installent et utilisent OpenManage Enterprise pour ces types de fonctionnalités de gestion du cycle de vie.

Remarque : Utiliser le plug-in Services pour OpenManage Enterprise activera nos fonctionnalités d'alerte, de création automatique de dossiers, d'expédition automatique et de collecte de télémétrie pour les serveurs PowerEdge avec un contrat de support actif. Toutefois, le plug-in Services n'active pas les fonctionnalités d'envoi de code de mise à niveau et d'accès au support à distance pour les systèmes gérés.

27. Quand dois-je utiliser le plug-in Services plutôt que le plug-in AIOps dans mon environnement OpenManage Enterprise ? Est-ce que je bénéficie d'une création de dossiers de support proactive et automatisée avec le plug-in AIOps ?

OpenManage Entreprise est une solution d'infrastructure de Dell qui facilite la gestion du cycle de vie de milliers de serveurs PowerEdge sur une seule console. Le tableau ci-dessous explique l'utilisation et les fonctionnalités du plug-in Services par rapport au plug-in AIOps.

Nous vous recommandons d'activer ***à la fois*** le plug-in Services et le plug-in AIOps pour tirer pleinement parti de leurs fonctionnalités respectives à partir de la console OpenManage Enterprise.

Aperçu des fonctionnalités et cas d'utilisation		
Plug-in	OpenManage Entreprise **Plug-in Services**	OpenManage Entreprise **Plug-in AIOps**
Quand l'utiliser	À activer lorsque vous souhaitez **les fonctionnalités de support proactives automatisées**	À activer lorsque vous souhaitez **les fonctionnalités du tableau de bord Dell AIOps basé sur le Cloud**
Fonctionnalités du plug-in	Offre des fonctionnalités d'alerte, de création automatique de dossiers, d'expédition automatique de pièces et de collecte de télémétrie	Permet la surveillance de l'intégrité et les informations prédictives sur les insuffisances de capacité, les anomalies de performances, les risques liés à la cybersécurité et la durabilité
Fonctionnalités activées pour	Les actifs avec un contrat de support actif, y compris les contrats ProSupport et ProSupport Plus. *Voir l'article Q21 de la base de connaissances.*	Les actifs avec des contrats ProSupport et ProSupport Plus
Configuration de la connectivité sécurisée expliquée	Remarque : Le client n'activera qu'une seule connexion, et non deux, dans son environnement. Une connexion TLS mutuelle sécurisée sera établie *entre* l'appliance OpenManage dans l'environnement du client et le back-end de Dell, basée sur la technologie Secure Connect Gateway.	
Élément clé à retenir	Si vous activez uniquement le plug-in Services, vous ne bénéficiez pas des fonctionnalités du plug-in AIOps. Si vous activez uniquement le plug-in AIOps, vous ne bénéficiez pas des fonctionnalités du plug-in Services. **Pratiques d'excellence recommandées : activez les deux plug-ins.**	

28. Qu'est-ce que Dell Connectivity Client qui s'affiche sur certains de mes systèmes PowerEdge ? Est-il compatible avec la technologie Secure Connect Gateway ?

Certains modèles de serveurs PowerEdge livrés avec iDRAC incluent un plug-in iDRAC (integrated Dell Remote Access Controller) appelé Dell Connectivity Client. Lisez les Questions fréquentes pour obtenir des informations spécifiques aux produits et aux régions. Ce client permet une connexion directe de l'iDRAC aux services back-end Dell et fournit une télémétrie en continu à l'aide de l'infrastructure OpenTelemetry.

- **Remarque** : Les clients doivent explicitement choisir d'utiliser ou non Dell Connectivity Client pendant le processus de vente, car cette configuration de produit PowerEdge est pré-activée par Dell.

À l'heure actuelle, Dell Connectivity Client ne peut pas se connecter aux éditions Virtual, Container ou Application d'une passerelle Secure Connect Gateway ni au plug-in Services pour OpenManage Enterprise.

La réponse à la question 28 continue à la page suivante…

28 (suite). Qu'est-ce que Dell Connectivity Client qui s'affiche sur certains de mes systèmes PowerEdge ? Est-il compatible avec la technologie Secure Connect Gateway ?

Si vous utilisez déjà une passerelle Secure Connect Gateway ou le plug-in Services pour les systèmes PowerEdge de votre environnement :

- Vous pouvez continuer à utiliser ces configurations existantes et *n'avez pas besoin* de reconnecter ces systèmes PowerEdge à Dell via Dell Connectivity Client. Toutefois, *vous devez prendre des mesures* pour désactiver Dell Connectivity Client pour ces systèmes PowerEdge. Lisez ce guide pour désactiver la configuration Dell Connectivity Client.

Si votre entreprise a besoin d'une connexion sécurisée unique pour se conformer aux stratégies de sécurité telles qu'une connexion de passerelle, la procédure suivante est recommandée :

- Vous téléchargez et installez la version appropriée des éditions Virtual, Container ou Application pour Secure Connect Gateway ou le plug-in Services pour OpenManage Enterprise.
- En outre, vous devez prendre des mesures pour désactiver Dell Connectivity Client pour ces systèmes PowerEdge. Vous connecterez ensuite ces systèmes à la passerelle ou via OpenManage Enterprise pour une surveillance conformément à nos guides techniques. En savoir plus sur ces options de déploiement technologique.

Informations générales

29. Où puis-je trouver des informations sur les politiques d'alerte pour Secure Connect Gateway ? À quel moment les dossiers de support prédictif sont-ils ouverts pour les pannes matérielles ?

Notre politique d'alerte Secure Connect Gateway fournit des informations sur les alertes qui ouvrent des dossiers d'incidents auprès du support technique Dell Technologies. Les clients qui utilisent Secure Connect Gateway recevront uniquement des alertes relatives à la création automatique de dossiers d'incidents prédictifs pour le matériel du serveur (disque dur, fond de panier et extenseurs) sur les systèmes dotés des services ProSupport Plus. Les alertes prédictives sont basées sur les collectes planifiées soumises à Dell Technologies.

30. 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 comptes et profils d'identification. Les comptes d'identification permettent aux administrateurs d'ajouter une authentification par type de produit. En outre, les profils permettent à plusieurs administrateurs qui diffèrent selon la fonction ou la région de gérer leurs comptes spécifiques. Les produits nécessitant des informations d'identification incluent les serveurs PowerEdge, les systèmes 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 fonctionnalité très intéressante, 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. Nous sommes intégrés au leader du marché CyberArk : les API CyberArk Conjur et les produits CyberArk Credential Provider sont actuellement pris en charge. Microsoft Azure Key Vault et HashiCorp Credential Vault sont également 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

31. Quelles sont les principales fonctionnalités du mode maintenance ?

Une « tempête d'événements » se produit lorsque des alertes matérielles se produisent à la chaîne, excédant la limite du nombre d'alertes prédéfini. Dans ce scénario, Secure Connect Gateway interrompt le traitement des alertes pour les appareils spécifiques qui ont déclenché la tempête d'événements. Tous les autres appareils continueront d'être surveillés par Secure Connect Gateway à la recherche d'alertes validées susceptibles de créer des dossiers de support.

En outre, les utilisateurs ont désormais la possibilité d'activer manuellement la maintenance sur un ou plusieurs appareils dans le système. Cela peut être utilisé pour une opération de maintenance planifiée et déployée lorsque vous ne souhaitez pas que Secure Connect Gateway surveille ces appareils. Une fois que les activités de maintenance planifiées sont terminées, vous pouvez désactiver manuellement le mode de maintenance pour signaler à Secure Connect Gateway de reprendre sa surveillance.

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

Oui. Vos préférences de notification par e-mail peuvent être personnalisées depuis l'interface utilisateur de Secure Connect Gateway, sous l'onglet Paramètres. Consultez le guide de l'utilisateur pour plus de détails.

33. 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.

34. 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.

35. Comment ce logiciel de connectivité est-il utilisé pour le portail Dell AIOps ?

Dell AIOps (anciennement APEX AIOps Infrastructure Observability et CloudIQ) est une solution d'observabilité et de gestion basée sur le Cloud et optimisée par l'IA, conçue pour optimiser l'infrastructure Dell.

Elle fournit des informations en temps réel pour améliorer les performances de l'infrastructure, renforcer la cybersécurité, favoriser le développement durable et soutenir la planification proactive. Grâce à sa plateforme intuitive et son assistant d'IA générative, Dell AIOps vous aide à réduire les risques, améliorer l'efficacité et simplifier les opérations IT.

- 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 de Dell AIOps.

36. Puis-je voir et gérer mes produits d'infrastructure Dell connectés avec des contrats de support actifs sur le portail TechDirect ?

Non, vous ne pouvez pas afficher ou gérer les produits d'infrastructure Dell connectés dans TechDirect. Notre logiciel de connectivité n'est pas intégré à TechDirect. Les données d'alerte et les dossiers de support automatisés pour les systèmes Dell connectés ne sont donc pas pris en charge ou visibles dans le tableau de bord du portail.

Toutefois, vous pouvez accéder et gérer les détails des dossiers de support automatisés pour les systèmes Dell connectés via les options de passerelle, de connexion directe et de plug-in sur le site de support en ligne et dans le tableau de bord analytique MyService360.