

Connectivité pour les systèmes d'entreprise

Table des matières

Informations générales

1. Qu'est-ce que la technologie de Passerelle de connexion sécurisée 5.x ? Remplace-t-elle les solutions SupportAssist Enterprise et Secure Remote Services ?
2. Existe-t-il d'autres méthodes de connexion outre l'utilisation de la Passerelle de connexion sécurisée ?
3. Est-il possible de continuer à utiliser la technologie SupportAssist Enterprise et Secure Remote Services ? Quand ces solutions seront-elles supprimées ?
4. Quelle est l'option de déploiement de la Passerelle de connexion sécurisée appropriée à mon environnement ?
5. Quels sont les logiciels recommandés pour mon environnement et les exigences minimales ?
6. Quelle version de SupportAssist Enterprise ou de Secure Remote Services doit être exécutée sur mon système afin de procéder à la mise à niveau vers la Passerelle de connexion sécurisée 5.x ?
7. Quelles sont les fonctionnalités de support automatisées disponibles avec la couverture ProSupport Enterprise Suite ?
8. Comment la Passerelle de connexion sécurisée permet-elle de gagner du temps lors du dépannage ?
9. Dois-je inscrire mon appareil équipé de la Passerelle de connexion sécurisée 5.x auprès de Dell Technologies ?
10. Comment obtenir de l'aide pour le déploiement de la technologie de Passerelle de connexion sécurisée ?
11. Si je rencontre des problèmes, comment puis-je contacter le support technique ?

Fonctionnalités générales

12. Où puis-je trouver des informations sur les politiques d'alerte pour la Passerelle de connexion sécurisée ? Quand les incidents de support prédictifs sont-ils ouverts pour les pannes matérielles ?
13. Comment puis-je accéder aux données relatives aux alertes automatisées de Dell dans mon tableau de bord, sous *Connect and Manage* dans le portail TechDirect ?
14. Que dois-je savoir sur les fonctions de gestion des informations d'identification dans la Passerelle de connexion sécurisée ?
15. Quelles sont les principales fonctionnalités du mode maintenance ?
16. Quelles sont les options disponibles si j'ai entre un et trois serveurs et que je ne souhaite pas installer la Passerelle de connexion sécurisée ou le plug-in de service pour OpenManage Enterprise ?

Fonctionnalités générales (suite)

17. Qu'advient-il des fonctions de la Passerelle de connexion sécurisée lorsque la couverture ProSupport Enterprise Suite ou ProSupport One for Data Center sur mon système surveillé arrive à expiration ?
18. La Passerelle de connexion sécurisée me permet-elle de définir des préférences de notification par e-mail ?
19. Quelles sont les langues prises en charge pour le tableau de bord de gestion de la connectivité sur site dans la Passerelle de connexion sécurisée ?
20. Où puis-je afficher les notifications d'intervention lorsque mes appareils sont connectés ?
21. Quels produits ont des capacités d'accès distant gérées par la Passerelle de connexion sécurisée ?
22. Qu'est-ce que le service Policy Manager pour la Passerelle de connexion sécurisée ?
23. Comment bien démarrer avec les API REST ?

Fonctionnalités principales : environnement OpenManage Enterprise et serveurs PowerEdge

- 24. Quels systèmes sont pris en charge par le plug-in de connectivité pour OpenManage Enterprise ?
- 25. Quelles sont les conditions préalables pour la surveillance de la connectivité des appareils PowerEdge ?
- 26. Comment la connectivité des services complète-t-elle la surveillance du cycle de vie de la gestion du datacenter par OpenManage Enterprise ?

Informations relatives à la sécurité

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

Informations générales

1. Qu'est-ce que la technologie de Passerelle de connexion sécurisée 5.x ? Remplace-t-elle les solutions SupportAssist Enterprise et Secure Remote Services ?

La technologie de [Passerelle de connexion sécurisée 5.x](#) est la solution de connectivité consolidée de nouvelle génération de Dell Technologies Services. Elle remplace les solutions existantes, SupportAssist Enterprise et Secure Remote Services, dont les fonctionnalités sont intégrées dans la technologie de Passerelle de connexion sécurisée.

La technologie de Passerelle de connexion sécurisée 5.x est un logiciel de support IT et de surveillance à distance livré sous forme d'appliance et d'application autonome. Elle fournit une solution unique pour l'ensemble de votre gamme Dell, prenant en charge les serveurs, la mise en réseau, le stockage des données, la protection des données, les solutions hyperconvergées et convergées. De plus, cette version apporte les avantages suivants :

- Un aperçu des problèmes les plus critiques
- La résolution accélérée des problèmes avec un accès distant et une communication bidirectionnelle sécurisée entre Dell Technologies et l'environnement du client
- Une installation et un enregistrement uniques pour le datacenter
- Une recommandation pour le téléchargement et l'installation de l'appliance VMware Skyline Collector lorsque SupportAssist identifie des clusters vCenter dans l'environnement
 - Cela sera uniquement recommandé aux clients qui n'ont pas encore installé Skyline. Skyline Collector est seulement proposé aux clients couverts par VMware Premier ou Production
- Un intérêt continu porté à la sécurité avec un nouveau logiciel Policy Manager qui comprend des fonctionnalités avancées d'audit et de contrôle, le protocole MQTT et les nouveaux processus de développement les plus performants
- L'amélioration des performances et de l'évolutivité avec la passerelle qui gère davantage de données et d'actions de télémétrie sur l'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

Cette technologie est disponible pour les clients de connectivité Dell Technologies, nouveaux et actuels, disposant d'une garantie ou d'un contrat pour un niveau de service de ProSupport Enterprise Suite.

Les clients actuels qui utilisent nos plates-formes de connectivité existantes, Secure Remote Services 3.x, ainsi que SupportAssist Enterprise v4.x et v2.x, peuvent facilement effectuer une mise à niveau vers notre toute dernière technologie, la Passerelle de connexion sécurisée, avec un minimum d'interruptions.

Les clients sont vivement encouragés à mettre à niveau proactivement leur connectivité d'entreprise afin d'éviter les interruptions du support automatisé et intelligent de leurs systèmes.

Reportez-vous à la question 3 pour plus d'informations sur la fin de vie des solutions existantes et à la question 6 pour obtenir des conseils sur les mises à niveau.

2. Existe-t-il d'autres méthodes de connexion outre l'utilisation de la Passerelle de connexion sécurisée ?

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

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.

3. Est-il possible de continuer à utiliser la technologie SupportAssist Enterprise et Secure Remote Services ? Quand ces solutions seront-elles supprimées ?

Si vous utilisez une technologie de support pour la première fois, ne téléchargez pas et n'utilisez pas ces anciennes technologies.

Récapitulatif des solutions technologiques existantes

SupportAssist Enterprise 4.x	SupportAssist Enterprise v2.x	Secure Remote Services (SRS) version 3.x (anciennement ESRS)
Pour les serveurs et les systèmes de stockage, de mise en réseau et CI/HCI. Fourni en tant qu'application autonome ou avec la console de gestion leader sur le marché, OpenManage Enterprise.	Pour les serveurs et les systèmes de stockage et de mise en réseau. Fourni en tant qu'application autonome ou avec les principales consoles de gestion, OpenManage Essentials, OpenManage Enterprise ou Microsoft System Center Operations Manager (SCOM). Aucune stratégie de mise à niveau directe de SupportAssist Enterprise 2.x vers 4.x.	Pour les systèmes de stockage, de protection des données et CI/HCI. Déployé en tant qu'appliance virtuelle ou système conteneurisé. Aucune stratégie de mise à niveau directe de Secure Remote Services vers SupportAssist Enterprise 4.x.

Dates d'entrée en vigueur de la fin de vie (EOSL) pour les solutions existantes :

- Retrait de **SupportAssist Enterprise 2.x et 4.x** le 31 juillet 2022.
- Retrait de **Secure Remote Services 3.x** pour tous les produits Dell le 15 juin 2023, à deux exceptions près. Pour les clients disposant de produits PowerStore et Unity qui utilisent une connexion directe, nous retirerons Secure Remote Services 3.x en juin 2024.

À la date d'entrée en vigueur, toutes les versions de la solution de connectivité spécifiée atteindront leur fin de vie. Par conséquent, le support (y compris les mesures correctives et l'atténuation des failles de sécurité) de la solution sera interrompu. La solution de remplacement est la nouvelle Passerelle de connexion sécurisée.

- **Remarque :** Les fonctionnalités proactives et prédictives des solutions de connectivité existantes pour les produits Dell seront interrompues, sauf si la mise à niveau vers la technologie de remplacement est en place.

À l'approche de la date de fin de vie d'une solution, Dell Technologies Services enverra un e-mail de notification aux clients concernés pour leur annoncer la fin du support et de la maintenance.

Pour ceux qui utilisent Secure Remote Services 3.x, ainsi que SupportAssist Enterprise v4.x et v2.x :

[Les stratégies de mise à niveau sans déplacement facilitent l'adoption de la technologie de Passerelle de connexion sécurisée 5.x](#) avec un minimum d'interruptions. Lancez-vous en cliquant sur les liens de mise à niveau dans le tableau de bord de gestion de la passerelle.

Ressources : [Démo interactive](#) | Vidéos techniques : éditions [Application](#) | [Appliance virtuelle](#)

4. Quelle est l'option de déploiement de la Passerelle de connexion sécurisée appropriée à mon environnement ?

Utilisez le tableau pour sélectionner l'option appropriée à votre environnement. Vous devez vérifier la matrice de support du produit pour la Passerelle de connexion sécurisée ou consulter la page du support produit sur Dell.com/Support. La version Application est plus adaptée aux petits clients ne disposant pas d'un environnement virtualisé et utilisant le matériel et les logiciels pris en charge ci-dessous.

Connectez-vous via la technologie de passerelle pour surveiller tous les appareils en un seul endroit

Solutions de passerelle intégrées	Matériel et logiciels pris en charge*
Passerelle de connexion sécurisée 5.x - Virtual Appliance Edition <i>Pour VMware</i> <i>Pour Microsoft Hyper-V</i>	Gamme complète de produits Dell EMC : stockage des données, serveurs, mise en réseau, CI/HCI et protection des données
Passerelle de connexion sécurisée 5.x - Application Edition <i>Gestion de Windows Enterprise sur des serveurs</i> <i>Gestion Linux sur les serveurs</i>	PowerEdge, iDRAC, PowerSwitch, Webscale, PeerStorage, EqualLogic, Compellent, Fluid File System (FluidFS), PowerVault
Plug-in de services pour OpenManage Enterprise <i>Pour votre environnement OpenManage Enterprise</i>	Serveurs PowerEdge
* Remarque : Notre technologie permet la connectivité avec VMware Skyline pour les serveurs PowerEdge exécutant vCenter	

Connexion directe pour certains matériels Dell EMC

- Intégration de la connectivité dans l'environnement d'exploitation du produit Dell EMC
- Approprié pour le déploiement hétérogène de plusieurs produits matériels Dell EMC
- Connexion directe à Dell Technologies ou via le serveur de la Passerelle de connexion sécurisée

5. Quels sont les logiciels recommandés pour mon environnement et les exigences minimales ?

[Passerelle de connexion sécurisée - Virtual Edition](#) :

Il existe des versions pour :

- Environnement VMware
- Environnement Microsoft Hyper-V

Passez en revue la configuration minimale requise pour l'installation et l'utilisation du logiciel de la Passerelle de connexion sécurisée. [Téléchargez la documentation et toutes les ressources](#) sur Dell.com/Support.

[Passerelle de connexion sécurisée - 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)

Passez en revue la configuration minimale requise pour l'installation et l'utilisation du logiciel. [Téléchargez la documentation et toutes les ressources](#) sur Dell.com/Support.

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

- Les nouveaux utilisateurs doivent tout d'abord créer un compte d'entreprise sur Dell.com/Support. Une fois sur la page de téléchargement de la Passerelle de connexion sécurisée vous serez invité à vous connecter et à télécharger le logiciel.
- Lorsque vous avez terminé, connectez-vous avec les informations d'identification de votre compte à la page du support produit de la Passerelle de connexion sécurisée sur Dell.com/Support.
- Assurez-vous de saisir un emplacement de 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.

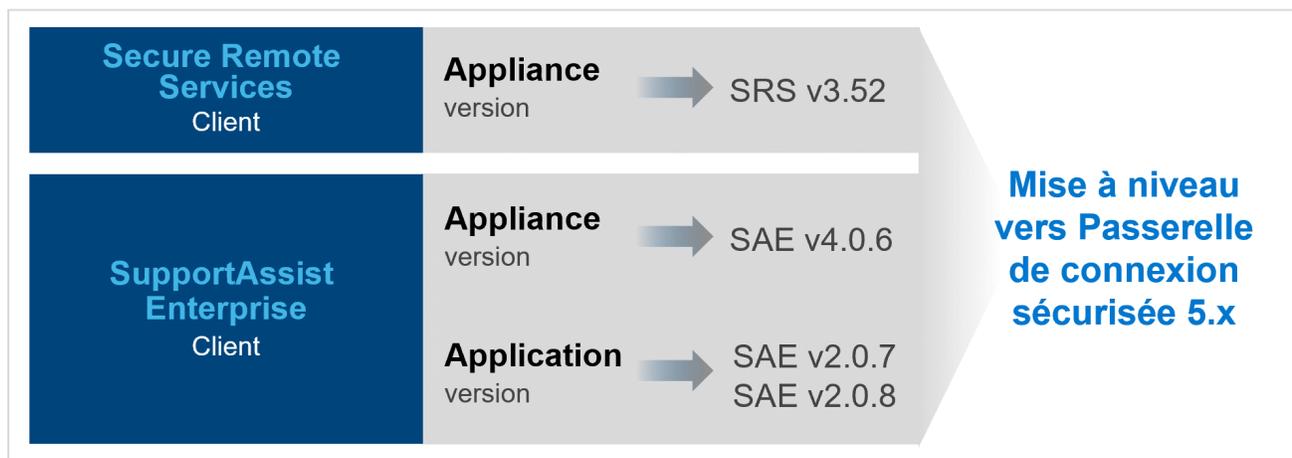
Découvrez la technologie : lancez notre [démonstration technique interactive](#)

- *Couvre les nouvelles installations des éditions Application et Virtual Appliance, la configuration des comptes d'entreprise (incluse dans les modules 1 et 2), les mises à niveau à partir de solutions existantes, les fonctionnalités du tableau de bord de gestion de la passerelle et le Policy Manager (Virtual Edition uniquement).*

Besoin d'aide ? Interrogez nos experts sur le [forum consacré à la Passerelle de connexion sécurisée](#)

6. Quelle version de SupportAssist Enterprise ou de Secure Remote Services doit être exécutée sur mon système afin de procéder à la mise à niveau vers la Passerelle de connexion sécurisée 5.x ?

Vous devez vous assurer que votre matériel ou logiciel Dell exécute les versions suivantes de SupportAssist Enterprise ou de Secure Remote Services. Vous recevrez un message vous invitant à effectuer une mise à niveau vers la [Passerelle de connexion sécurisée 5.x](#) dans votre interface utilisateur Web.



Conseil : Consultez les étapes du Module 3 *Upgrade from Secure Remote Services 3.52 (Mise à niveau à partir de Secure Remote Services 3.52)* et du Module 4 *Upgrade from SupportAssist Enterprise 2.0.7 & 2.0.8 (Mise à niveau à partir de SupportAssist Enterprise 2.0.7 et 2.0.8)* dans la [démonstration interactive](#)

7. Quelles sont les fonctionnalités de support automatisées disponibles avec la couverture ProSupport Enterprise Suite ?

Fonctionnalités	Basic	ProSupport	ProSupport Plus
Détection des problèmes et collecte des informations sur l'état des systèmes automatisées	•	•	•
Création de dossiers d'incidents et envoi de notification proactifs et automatisés		•	•
Détection prédictive des problèmes pour la prévention des pannes ¹			•

1. La détection des défaillances via l'analyse prédictive inclut les disques durs de serveur et les fonds de panier lorsqu'ils sont connectés via la Passerelle de connexion sécurisée

En savoir plus sur l'offre [Enterprise Support Services](#) pour l'intégration des services ProSupport Enterprise Suite.

8. Comment la Passerelle de connexion sécurisée permet-elle de gagner du temps lors du dépannage ?

Notre technologie de connectivité détecte automatiquement les problèmes, recueille des informations sur l'état du système, lance des alertes et contacte Dell Technologies. Vous gagnez du temps en termes de collecte des informations sur l'état du système, de création d'incidents et d'implication avec Dell Technologies. Vous pouvez également utiliser la passerelle de connexion sécurisée pour exécuter des collectes automatiques ou à la demande et pour nous envoyer automatiquement les informations sur l'état du système pour la création proactive de dossiers d'incidents. En fonction du problème et de vos préférences, la passerelle de connexion sécurisée a également la possibilité de lancer une résolution à distance avec un accès distant sécurisé, ainsi qu'une communication bidirectionnelle sécurisée entre vous et Dell Technologies.

9. Dois-je inscrire mon appareil équipé de la Passerelle de connexion sécurisée 5.x auprès de Dell Technologies ?

Oui. Pour utiliser la Passerelle de connexion sécurisée et bénéficier d'une sécurité optimale, vous devez vous inscrire auprès de Dell Technologies. Utilisez votre compte d'entreprise pour vous connecter à la page de téléchargement, générer une clé d'accès et un code PIN. Utilisez votre clé d'accès et votre code PIN pour activer votre Passerelle de connexion sécurisée. Les clients qui ne disposent pas d'un compte d'entreprise devront fournir des informations supplémentaires sur leur entreprise et leurs produits. Le client pourra poursuivre une fois le processus de vérification effectué.

10. Comment obtenir de l'aide pour le déploiement de la technologie de Passerelle de connexion sécurisée ?

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](#).

Conseil : Vous pouvez lancer et découvrir notre [démonstration technique interactive](#)

- *Couvre les nouvelles installations des éditions Application et Virtual Appliance, la configuration des comptes d'entreprise (incluse dans les modules 1 et 2), les mises à niveau à partir de solutions existantes, les fonctionnalités du tableau de bord de gestion de la passerelle et le Policy Manager (Virtual Edition uniquement).*

Pour ceux qui souhaitent obtenir de l'aide, la [suite de services ProDeploy Enterprise Suite](#) comprend l'activation et la configuration de la Passerelle de connexion sécurisée. Les clients disposant de la [couverture ProSupport Plus](#) se voient attribuer un Service Account Manager (SAM), qui peut les aider en cas de questions sur l'installation et l'inscription. Sinon, contactez le support technique de Dell Technologies pour obtenir de l'aide.

11. Si je rencontre des problèmes, comment puis-je contacter le support technique ?

Si vous rencontrez des problèmes avec le support en ligne sur Dell.com ou avec la Passerelle de connexion sécurisée, rendez-vous sur notre page de [support administratif à partir de cet emplacement](#) pour obtenir de l'aide. Sélectionnez la catégorie qui se rapproche le plus de votre problème et renseignez les détails à l'invite. Si vous avez besoin d'une assistance immédiate pour un problème de support technique, contactez-nous à partir de [cet emplacement](#). Veuillez contacter votre Service Account Manager (le cas échéant).

Fonctionnalités générales

12. Où puis-je trouver des informations sur les politiques d'alerte pour la Passerelle de connexion sécurisée ? Quand les incidents de support prédictifs sont-ils ouverts pour les pannes matérielles ?

La [politique d'alerte de la Passerelle de connexion sécurisée](#) fournit des informations sur les alertes qui ouvrent des dossiers d'incidents auprès du support technique de Dell Technologies. Les clients qui utilisent la passerelle de connexion sécurisée 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.

13. Comment puis-je accéder aux données relatives aux alertes automatisées de Dell dans mon tableau de bord, sous *Connect and Manage* dans le portail TechDirect ?

Dans le tableau de bord en ligne du portail TechDirect, sous l'onglet *Connect and manage*, vous pouvez gérer les alertes et les ressources d'entreprise. Dans cet exemple, l'administrateur informatique peut définir des règles pour passer en revue les alertes automatisées pour la création de dossiers de support ou l'expédition de pièces, et déterminer s'il souhaite les transférer vers Dell Technologies.

Exigences importantes relatives à la connectivité dans Intelligence de service pour les données : le client doit intégrer les données d'alerte à ce tableau de bord dans le cadre de la configuration de la passerelle sur site. Cela s'applique aux éditions Gateway et au plug-in pour l'environnement OpenManage Enterprise.

Remarque : Cette fonctionnalité est disponible pour les systèmes PowerEdge, iDRAC, PowerSwitch, Webscale, PeerStorage, EqualLogic, Compellent, Fluid File System (FluidFS), PowerVault et PowerStore qui utilisent SupportAssist Enterprise 2.x, le plug-in SupportAssist OpenManage Enterprise 1.x, le plug-in de services pour OpenManage Enterprise 1.x, SupportAssist Enterprise 4.x et/ou la connectivité de la Passerelle de connexion sécurisée 5.x. Veuillez à vérifier les étapes d'intégration obligatoires dans le guide de l'utilisateur et le manuel d'installation du produit.

Autre : les alertes relatives aux appareils connectés à la technologie Secure Remote Services ne sont pas prises en charge dans le tableau de bord *Enterprise Assets and Alerts* de TechDirect.

14. Que dois-je savoir sur les fonctions de gestion des informations d'identification dans la Passerelle de connexion sécurisée ?

La Passerelle de connexion sécurisée offre la flexibilité d'ajouter plusieurs profils et comptes d'identification. Les comptes d'identification permettent aux administrateurs d'ajouter une authentification en fonction du type de produit. En outre, les profils permettent à plusieurs administrateurs, qui diffèrent par fonction ou zone géographique, de gérer leurs comptes spécifiques. Les produits pour lesquels les informations d'identification sont nécessaires sont : serveurs PowerEdge, iDRAC, Compellent, systèmes de mise en réseau, systèmes de la série PS, systèmes de la série MD et systèmes Webscale.

Conseil : Obtenez un aperçu de ces fonctionnalités dans le Module *M5.3 Device Management (Gestion des périphériques)* dans la [démonstration interactive](#)

15. 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, la Passerelle de connexion sécurisée 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 la Passerelle de connexion sécurisée 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 la passerelle de connexion sécurisée surveille ces appareils. Une fois que les activités de maintenance planifiées sont terminées, vous pouvez désactiver manuellement le mode de maintenance pour signaler à la Passerelle de connexion sécurisée de reprendre sa surveillance.

16. Quelles sont les options disponibles si j'ai entre un et trois serveurs et que je ne souhaite pas installer la Passerelle de connexion sécurisée ou le plug-in de service pour OpenManage Enterprise ?

Pour les clients disposant de serveurs PowerEdge 14G et 15G, la connectivité basée sur la technologie SupportAssist est intégrée en usine sur votre serveur. Pour démarrer le support proactif et prédictif automatisé, activez iDRAC Service Module (iSM) et inscrivez SupportAssist dans la console iDRAC.

17. Qu'advient-il des fonctions de la Passerelle de connexion sécurisée lorsque la couverture ProSupport Enterprise Suite ou ProSupport One for Data Center sur mon système surveillé arrive à expiration ?

Si votre contrat de service ProSupport Enterprise Suite ou ProSupport One for Data Center arrive à expiration, la fonction de création automatique d'incidents sera désactivée. La Passerelle de connexion sécurisée continuera toutefois à exécuter les collectes de l'état du système automatisé. Si vous effectuez une mise à niveau ou une extension de votre contrat sur un système (numéro de série), la création automatique d'incidents est réactivée automatiquement sur ce système.

18. La Passerelle de connexion sécurisée me 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 la Passerelle de connexion sécurisée, sous l'onglet Paramètres. Consultez [le guide de l'utilisateur pour plus de détails](#).

19. Quelles sont les langues prises en charge pour le tableau de bord de gestion de la connectivité sur site dans la Passerelle de connexion sécurisée ?

L'interface logicielle de la Passerelle de connexion sécurisée 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'un incident de demande de service. Remarque : Certaines notifications par e-mail ne sont pas traduites dans la langue locale, en fonction des limitations du système d'exploitation.

20. Où puis-je afficher les notifications d'intervention lorsque mes appareils sont connectés ?

À partir du tableau de bord pour la gestion des ressources d'entreprise et des alertes, sous *Connect and manage*, dans le portail TechDirect :

- Vous pouvez modifier vos préférences d'expédition pour les serveurs Dell et les systèmes de stockage et de mise en réseau éligibles.
- Exigences importantes relatives à la connectivité pour les données : Le client doit intégrer les données d'alerte à ce tableau de bord dans le cadre de la configuration de la passerelle sur site. Cela s'applique aux éditions Gateway et au plug-in pour l'environnement OpenManage Enterprise. Référez-vous à la question 13 de ce document.

À partir du tableau de bord d'analytique du portail MyService360 :

- Vous pouvez afficher les notifications d'expédition pour les solutions Dell de stockage, de protection des données et CI/HCI éligibles

21. Quels produits ont des capacités d'accès distant gérées par la Passerelle de connexion sécurisée ?

Les produits Dell de stockage des données, de protection des données et CI/HCI ont des capacités d'accès distant. Les agents de support technique autorisés utilisent une authentification à deux facteurs requise pour accéder à distance à des périphériques gérés afin de dépanner et de résoudre les problèmes. Toutes les sessions distantes sont auditées et il est possible d'accéder aux détails depuis la console de gestion sur site de la Passerelle de connexion sécurisée, dans la section Audit. Pour des fonctions supplémentaires de contrôle et d'audit avancé, les clients peuvent configurer un serveur de gestion des règles, ce qui permet de bloquer ou d'autoriser toutes les sessions d'accès distant.

22. Qu'est-ce que Policy Manager pour la Passerelle de connexion sécurisée ?

Policy Manager pour la Passerelle de connexion sécurisée est un logiciel distinct et complémentaire qui peut être installé pour des fonctions d'audit avancées. À l'aide du logiciel Policy Manager, vous pouvez définir des règles pour le support à distance, le transfert de fichiers et/ou les actions distantes pour les produits qui prennent en charge une ou plusieurs de ces capacités d'accès distant.

Conseil : Obtenez un aperçu de ces fonctionnalités dans le Module *M6 Virtual Edition – Policy Management (Gestion des règles)* dans la [démonstration interactive](#) et consultez les vidéos techniques d'instructions pour l'édition [Virtual Appliance](#).

23. Comment bien démarrer avec les API REST ?

Avec la Passerelle de connexion sécurisée, 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 dans [notre section documentation](#).

Fonctionnalités principales : environnement OpenManage Enterprise et serveur PowerEdge

24. Quels systèmes sont pris en charge par le plug-in de connectivité pour OpenManage Enterprise ?

Les serveurs et les boîtiers PowerEdge (12G à 15G) avec iDRAC et Chassis Management Controller (CMC), ainsi que les serveurs Linux sont pris en charge.

[En savoir plus sur les produits pris en charge et obtenir des ressources techniques.](#)

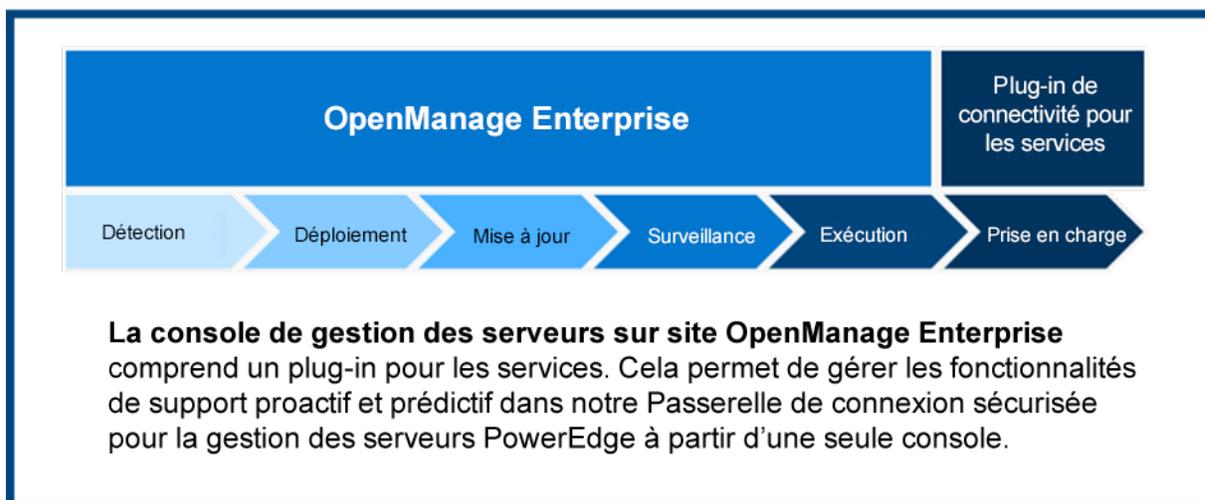
25. Quelles sont les conditions préalables pour la surveillance de la connectivité des appareils PowerEdge ?

Le plug-in pour OpenManage Enterprise et les éditions Gateway peuvent surveiller les serveurs PowerEdge 12G et versions plus récentes hors bande (lors de l'utilisation d'iDRAC7, iDRAC8 et iDRAC9), ainsi que les boîtiers PowerEdge. Pour plus d'informations, reportez-vous à la matrice de support pour l'appareil spécifique.

Les serveurs PowerEdge peuvent également être gérés intrabande à condition que l'agent OpenManage Server Administrator (OMSA) soit installé et en cours d'exécution sur l'appareil. La version recommandée de OMSA varie selon le système d'exploitation exécuté sur l'appareil.

26. Comment la connectivité des 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 de type « un à plusieurs » simple à utiliser. Elle facilite la gestion économique complète du cycle de vie pour les serveurs et boîtiers PowerEdge sur une seule console. Reportez-vous au diagramme ci-dessous pour comprendre comment le plug-in de connectivité pour OpenManage Enterprise vient compléter l'expérience OpenManage Enterprise pour le datacenter. Cette fonctionnalité est actuellement disponible via le plug-in OpenManage Enterprise SupportAssist 1.x et la dernière version de notre plug-in, OpenManage Services 1.x. [En savoir plus et trouver des ressources.](#)



Informations relatives à la sécurité

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

Téléchargez le [livre blanc sur la sécurité](#) pour découvrir comment la technologie de Passerelle de connexion sécurisée intègre la protection des données et la prévention des menaces dans une expérience de support automatisée et sécurisée.

Ce document traite des sujets suivants :

- **Collecte de données sur site sécurisée** : découvrez comment la Passerelle de connexion sécurisée agit en tant que courtier de communications sécurisé, permet aux clients de contrôler les exigences d'autorisation, d'utiliser 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.