Konnektivität für Dell Infrastruktursysteme

Inhaltsverzeichnis

Inhaltsverzeichnis – Fortsetzung

Einführung

1: Was ist die secure connect gateway-Technologieplattform?

Unsere secure connect gateway 5.x-Technologie ist die Konnektivitätssoftware der nächsten Generation von Dell Technologies Services.

Sie bietet **eine einzige Konnektivitätslösung für das Management Ihres gesamten Dell Infrastrukturportfolios**, d. h. Server, Netzwerke, Daten-Storage, Data Protection sowie konvergente und hyperkonvergente Lösungen (CI/HCI). Sie ersetzt außerdem die Legacy-Software SupportAssist Enterprise und Secure Remote Services, deren Funktionen in diese Technologie integriert sind.

Wir bieten **flexible Bereitstellungsoptionen, die vom Kunden installiert und aktualisiert werden können**. Mit einer Gatewayoption (bereitgestellt als virtuelle Appliance, eigenständige Anwendung oder Container-Edition), einer Direktverbindungsoption und einer Plug-in-Option können Sie auswählen, was für Ihre Umgebung am besten geeignet ist.

Unsere Technologie **– auch bekannt als Remote-IT-Support- und -Monitoringsoftware –** bietet Folgendes:

- Einblick in die kritischsten Probleme
- Beschleunigte Problembehebung durch Remotezugriff und sichere bidirektionale Kommunikation zwischen Dell Technologies und der Kundenumgebung
- Fortlaufende Fokussierung auf Sicherheit mit Policy-Manager-Software mit erweiterten Audit- und Kontrollfunktionen, dem erstklassigen MQTT-Protokoll und neuen Entwicklungsprozessen
- Verbesserte Performance und Skalierbarkeit mit dem Gateway, das noch mehr Telemetriedaten und Aktionen in Ihrer Dell Enterprise-Umgebung verarbeitet
- Eine verbesserte Erfahrung in der Webbenutzeroberfläche für unser Dashboard für das On-Premise-Konnektivitätsmanagement

Sobald Sie ein Dell Infrastrukturprodukt erworben haben und es mit einem Supportservicevertrag gebündelt ist, z. B. mit einem beliebigen Servicelevel der ProSupport Infrastructure Suite, können Sie diese Konnektivitätssoftware kostenlos einrichten. Es ist keine Lizenz erforderlich.

Wenn unsere Software die Systeme überwacht, bieten wir Ihnen unsere einzigartige Integration von intelligenterer KI, automatisiertem Support und Echtzeitanalysen.

2: Gibt es neben der Verwendung der Gatewayoption noch andere Möglichkeiten, eine Verbindung herzustellen?

Ja. Die secure connect gateway-Technologie wurde auch als Version mit Direktverbindung für ausgewählte Dell Hardware und als Plug-in implementiert.

Einige Dell Produkte können direkt mit dem Dell Technologies Backend verbunden werden und eignen sich für Kunden, die keine separate Software einrichten möchten. Weitere Informationen finden Sie in Ihrer Produktdokumentation. *Zusätzliche Details finden Sie in Frage 12.*

Kunden in einem PowerEdge-Rechenzentrum, die OpenManage nutzen, können jetzt für Warnmeldungen, den automatischen Versand und Erfassungsfunktionen eine Verbindung mit unserem Services-Plug-in für OpenManage Enterprise herstellen.

Erkunden Sie die Technologie: Besuchen Sie Dell.com, um mehr von unseren ExpertInnen zu erfahren und technische Ressourcen zu erhalten

Infografik mit wichtigen Links: Erste Schritte mit Konnektivität im Rechenzentrum

3: Wurde die Legacy-Software – SupportAssist Enterprise und Secure Remote Services – eingestellt?

Die **Virtuelle und Docker-Editionen von Secure Remote Services v3.x** wurden am 31. Januar 2024 vollständig stillgelegt. Der intelligente, automatisierte Support für die unterstützten Dell Storage-, Netzwerk- und CI-/HCI-Systeme wurde eingestellt.

- Hinweis: Für Kunden mit **Dell PowerStore- und Unity-Produkten, die eine Direktverbindung nutzen**, wird die Technologie am 31. Dezember 2024 eingestellt. Um Serviceunterbrechungen zu vermeiden, wird vor dem EOSL ein Update der Betriebsumgebung zur Verfügung gestellt.

SupportAssist Enterprise 4.x und 2.x wurden am 31. Juli 2022 stillgelegt. Der intelligente, automatisierte Support für Dell Server-, Storage-, Netzwerk- und/oder CI-/HCI-Systeme wurde eingestellt.

4: Handelt es sich um Software, die vom Kunden installiert und aktualisiert werden kann?

Ja. Sie können unsere Konnektivitätstechnologie ohne Unterstützung von Dell Technologies herunterladen und installieren.

Besuchen Sie die Dell Support-Website für die Gateway- und Plug-in-Softwareressourcen.

- **Tipp:** Sehen Sie sich unser interaktives technisches Demo (nur in englischer Sprache) an, um eine Vorschau der Installation, Registrierung und Verwendung der Gateway-Editionen und der Policy-Manager-Software zu erhalten.

5: Benötige ich eine Lizenz?

Es ist keine Softwarelizenz erforderlich. Um Ihre Software herunterzuladen und zu registrieren, müssen Sie sich jedoch unter Dell.com beim Support authentifizieren.

Funktionen und Mehrwert der Technologie

6: Inwiefern bietet die Verwendung von Konnektivitätssoftware einen Mehrwert für die Dell Supporterfahrung?

Unternehmen verwenden unsere Konnektivitätstools hauptsächlich zur Reduzierung von Ausfallzeiten in ihrer Umgebung, zur Verringerung des Aufwands für die Überwachung kritischer Probleme sowie zur Identifizierung und Behebung kleinerer Probleme, bevor sie zu größeren und kostspieligeren werden.

Die Einrichtung der Konnektivität verbessert die Supporterfahrung für Dell Infrastrukturprodukte mit Abdeckung durch Support Services, z. B. mit jedem beliebigen Servicelevel für die ProSupport Infrastructure Suite. Sobald unsere secure connect gateway-Technologie – die als Gateway-, Direktverbindungs- oder Plug-in-Option implementiert wird – die Systeme in Ihrer Umgebung überwacht, bieten wir Ihnen proaktiven, präventiven und in einigen Fällen vorausschauenden Support.

Daten sind das Herzstück unserer Konnektivitätstechnologie. **Wir nutzen Systemstatusdaten aus Kundenumgebungen und korrelieren diese mit Incident- und Engineering-Daten**, die über Jahre von Außendienst- und technischen Supportteams sowie von Komponentenherstellern gesammelt wurden. Mithilfe **fortschrittlicher KI-Modelle, einschließlich maschinellem Lernen**, kann unsere Konnektivitätstechnologie Muster finden und diese auf die Telemetrie- und Ereignisdaten anwenden, um genau das richtige Problem zu erkennen und darauf zu reagieren.

Unsere Technologie identifiziert Hardware- und Softwareprobleme, **erstellt einen Fall und initiiert den Kontakt von unserer Seite, um mit der Lösung eines Problems zu beginnen, bevor es zu einem kostspieligen Problem wird**. Je nach Art des Problems kann die Warnmeldung auch **einen automatischen Teileversand auslösen**, was einen schnelleren Erhalt von Hardwareteilen bedeutet.

Eine weitere großartige Funktion ist der **Remotesupport**, der in den meisten unserer Storage-, Data-Protection-, konvergenten und hyperkonvergenten Produkte (CI/HCI) enthalten ist. In diesem Szenario – wenn ein Fall auf unserer Seite eröffnet wird – und wir die Fehlerbehebung über den Remotesupport durchführen können, ermöglicht die Technologie eine sichere bidirektionale Kommunikation für autorisierte MitarbeiterInnen des technischen Supports, die remote auf verwaltete Geräte zugreifen, um Probleme zu diagnostizieren und zu beheben.

Wenn Sie Telemetriedaten zurück an Dell senden, **können die Verlaufsdaten Ihres Systems außerdem dazu beitragen, die Problemlösungszeit zu verkürzen**, wenn der Dell Support hinzugezogen wird. Wenn beispielsweise eine Warnmeldung an Dell zurückgesendet wird, können SupporttechnikerInnen eine Verbindung mit dem Gerät herstellen (basierend auf den vom Kunden festgelegten Policies), dann bestätigen, welche Maßnahmen ergriffen werden müssen, und dem Kunden einen Aktionsplan zur Verfügung stellen. So können beispielsweise Teile ausgetauscht werden, bevor sie tatsächlich ausfallen, wodurch letztendlich das Risiko von Ausfallzeiten minimiert wird.

Ein weiterer Vorteil der Remotesupportfunktionen sind **Remoteupgrades**. Diese sind ein großartiges Beispiel dafür, wie wir unsere sichere Verbindung nutzen. Bei vielen Produkten können Upgradecodes oder Sicherheitspatches für das Produkt direkt versendet werden, damit der Kunde sie nach Belieben anwenden kann. Alternativ können unsere Remote-Changemanagementteams das Upgrade von Anfang bis Ende planen und ausführen, ohne vor Ort zu sein.

Erfahren Sie mehr von unseren ExpertInnen:

- Podcast anhören (nur in englischer Sprache): Maximierung der Verfügbarkeit von Rechenzentren mit intelligentem Support
- Podcast anhören (nur in englischer Sprache): Maximierung der PowerEdge-Verfügbarkeit mit proaktivem, vorausschauendem Support

Kurze Videos ansehen (nur in englischer Sprache):

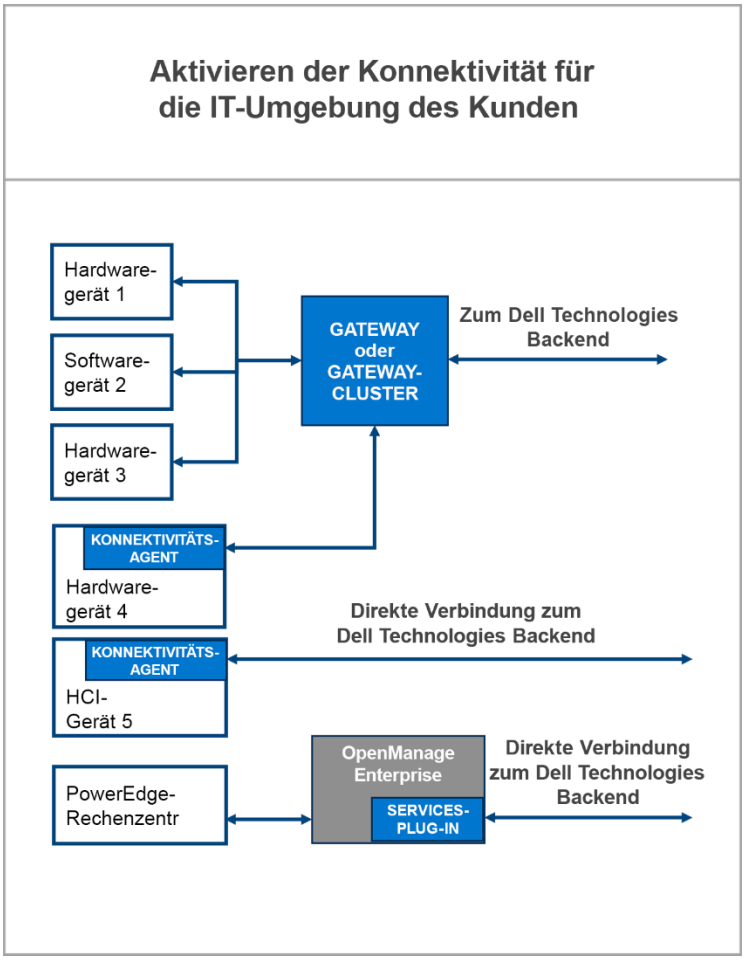
- Funktionen und Vorteile der Konnektivität
- Sicherheitsarchitektur und -funktionen

Optionen für die Technologiebereitstellung

7: Wie kann ich die Konnektivitätssoftware in meiner Umgebung bereitstellen und konfigurieren?

Mit unseren flexiblen Installationsoptionen – einer Gateway-, einer Direktverbindungs- und einer Plug-in-Option – können Sie die passende Lösung für Ihre Umgebung auswählen. Alle sind vom Kunden installierbar und aktualisierbar.

Mit der **secure connect gateway-Option** können Sie Ihre Dell Systeme mit dem Gateway verbinden, um mit Dell Technologies Services zu kommunizieren. Dies vereinfacht Ihre Firewall-/Netzwerkeinrichtung, sodass das Gateway die einzige Komponente ist, die eine ausgehende Verbindung über das Internet herstellt.



Für unsere Gatewayoption bietet Dell eine **Virtual Edition** für VMware- und Hyper-V-Umgebungen. Wir stellen außerdem **Container Editions** für Docker-, Podman- und Kubernetes-Umgebungen bereit. Für unsere kleineren Serverkunden bieten wir eine **Application Edition** mit Windows-/Linux-Versionen. *Siehe Fragen 8 bis 11.*

Kunden, die hohe Verfügbarkeit und Failover für ihre Systeme wünschen, können mehrere Gateways oder einen Cluster einrichten. Damit erhalten sie Redundanz, falls ein Gateway nicht verfügbar ist.

Die **Direktverbindungsoption** (die durch die Integration unserer Konnektivitätstechnologie in die Betriebsumgebung des Dell Produkts ermöglicht wird) ist für kleinere und nicht herkömmliche Kunden vorgesehen, die möglicherweise keine zusätzliche Software einrichten möchten. *Mehr dazu erfahren Sie in Frage 12.*

Schließlich haben wir für unsere Compute-orientierten Kunden das **Services-Plug-in für OpenManage Enterprise**, mit dem Sie eine einzige, sichere Direktverbindung für Ihre PowerEdge-Serverflotte herstellen können. *Mehr dazu erfahren Sie in den Fragen 13 und 23 bis 25.*

Infografik mit wichtigen Links: Erste Schritte mit Konnektivität im Rechenzentrum

7 (Fortsetzung): Wie kann ich die Konnektivitätssoftware in meiner Umgebung bereitstellen und konfigurieren?

Ermitteln Sie anhand der Tabelle unten die geeignete Option für Ihre Umgebung. Sehen Sie in der Produkt-Supportmatrix für secure connect gateway nach oder besuchen Sie die Supportseite für Hardwareprodukte unter Dell.com/Support. Die Application Edition eignet sich am besten für kleinere Kunden, die nicht über eine virtualisierte Umgebung verfügen und die unterstützte Dell Hardware und Software verwenden.

Verbindung zur Überwachung aller Geräte an einem Ort

Integrierte Lösungen	Unterstützte Hardware und Software
Secure Connect Gateway 5.x – Virtual Appliance Edition *für VMware und Microsoft HyperV* *Containerpakete: Docker, Podman, Kubernetes*	Gesamtes Dell Produktportfolio – Daten-Storage, Server, Netzwerke, CI/HCI und Data Protection
Secure Connect Gateway 5.x – Application Edition *Windows Enterprise-Management auf Servern* *Linux-Management auf Servern*	PowerEdge, iDRAC, PowerSwitch, Webscale, PeerStorage, EqualLogic, Compellent, Fluid File System (FluidFS), PowerVault
OpenManage Enterprise-Services-Plug-in *für Ihre OpenManage Enterprise-Umgebung*	PowerEdge-Server

Direktverbindung für ausgewählte Dell Hardware

- Integration von Konnektivität in die Betriebsumgebung von Dell Produkten – sehen Sie sich die Dell Produktsupportdokumentation an, um das spezifische Produktmodell und die Version zu überprüfen
- Geeignet für die heterogene Bereitstellung von mehreren Dell Hardwareprodukten
- Direkte Verbindung zu Dell Technologies oder über den secure connect gateway-Server

Infografik mit wichtigen Links: Erste Schritte mit Konnektivität im Rechenzentrum

8: Welche Gatewaysoftware wird für meine Umgebung empfohlen und welche Mindestanforderungen gelten?

Gatewaysoftware	
Secure Connect Gateway – Virtual Edition Es gibt Versionen für: • VMware-Umgebung/Microsoft HyperV-Umgebung • Containerpakete: Docker, Podman, Kubernetes Laden Sie die Dokumentation und alle Ressourcen von Dell.com/Support herunter.	Secure Connect Gateway – Application Edition Es gibt Versionen für: • Windows-Managementserver (überwacht sowohl Windows- als auch Linux-Geräte) • Linux-Managementserver (überwacht Linux-Geräte) Laden Sie die Dokumentation und alle Ressourcen von Dell.com/Support herunter.
Sehen Sie sich das interaktive technische Demo an, um technische Tipps zur Installation, Registrierung und Verwendung zu erhalten.	
Informieren Sie sich unbedingt über die Mindestanforderungen für die Installation und Verwendung der secure connect gateway-Software.	

Tipps für die ersten Schritte neuer NutzerInnen:

- Neue NutzerInnen müssen zuerst ein Enterprise-Geschäftskonto unter Dell.com/Support einrichten. Sie werden auf der secure connect gateway-Downloadseite aufgefordert, sich anzumelden und diesen Schritt abzuschließen.
- Melden Sie sich danach mit Ihren Kontozugangsdaten bei der secure connect gateway-Produktsupportseite unter Dell.com/Support an.
- Stellen Sie sicher, dass Sie den Standort der Software-installation eingeben. Dies hilft uns, eine bessere Supporterfahrung zu bieten.
- Beziehen Sie die richtige Edition für Ihre Umgebung. In diesem Schritt müssen Sie den Authentifizierungszugriffsschlüssel erstellen.

Hinweis: *Für diejenigen, die zum ersten Mal eine Verbindung herstellen, nimmt die Vorbereitung des Standorts die meiste Zeit in Anspruch – von einigen Tagen bis zu potenziell einigen Monaten, je nach Komplexität Ihrer Netzwerk- und Sicherheits-Policies. Ihre Sicherheits- und Netzwerkteams bitten möglicherweise um eine Produktüberprüfung vor der Implementierung.* Lesen Sie dazu unser Whitepaper zum Thema Sicherheit.

Erkunden Sie die Technologie: Besuchen Sie Dell.com, um mehr von unseren ExpertInnen zu erfahren und technische Ressourcen zu erhalten.

Benötigen Sie Hilfe? Stellen Sie unseren ExpertInnen beliebige Fragen über das Secure Connect Gateway-Forum.

9: Muss ich mein secure connect gateway-Gerät bei Dell Technologies registrieren?

Ja. Um secure connect gateway verwenden und erstklassige Sicherheit erhalten zu können, müssen Sie sich bei Dell Technologies registrieren.

> **Tipp:** Erfahren Sie, wie Sie ein Enterprise-Geschäftskonto einrichten. Sie sind ordnungsgemäß authentifiziert, wenn unter Dell.com/Support ein schwarzes Häkchen neben Ihrem Namen angezeigt wird.

Verwenden Sie Ihr Enterprise-Geschäftskonto, um sich bei der Downloadseite anzumelden sowie einen Zugriffsschlüssel und eine PIN zu generieren. Verwenden Sie Ihren Zugriffsschlüssel und Ihre PIN dann, um Ihr secure connect gateway zu aktivieren.

Kunden, die nicht über ein Geschäftskonto verfügen, werden nach zusätzlichen Informationen zu ihren Unternehmen und Produkten gefragt. Der Kunde kann fortfahren, nachdem er den Verifizierungsprozess durchlaufen hat.

10: Welche Gatewaytechnologie verfügt über Remotesupportfunktionen? Welche Produkte bieten Remotezugriffsfunktionen, die von secure connect gateway verwaltet werden?

Remotesupportfunktionen sind nur in der Virtual und Container Edition von secure connect gateway verfügbar, *nicht in der Application Edition*.

Daten-Storage-, Data-Protection- sowie konvergente und hyperkonvergente Produkte (CI/HCI) verfügen über Remotezugriffsfunktionen. Die PowerEdge- und PowerSwitch-Produkte können auch für Remotesupport in der On-Premise-Gateway-Managementbenutzeroberfläche über die Geräteübersicht aktiviert werden.

Autorisierte MitarbeiterInnen des technischen Supports verwenden eine erforderliche Zwei-Faktor-Authentifizierung für den Remotezugriff auf verwaltete Geräte, um Probleme zu diagnostizieren und zu lösen. Alle Remotesitzungen werden überprüft. Sie können auf die Details über die Managementkonsole des On-Premise-Gateways für secure connect gateway im Abschnitt „Audit“ zugreifen.

Für eine zusätzliche Kontrolle und erweiterte Auditingfunktionen können Kunden einen Policy-Management-server einrichten, der die Flexibilität bietet, alle Remotezugriffssitzungen zu blockieren oder zuzulassen.

11: Was ist die Policy-Manager-Software und wie wird sie für die Gatewayoption verwendet?

Der Policy-Manager für secure connect gateway ist eine separate und ergänzende externe Software, die für erweiterte Auditing- und Remotesteuerungsfunktionen installiert werden kann.

Mit dem Policy-Manager können Sie Policies für Remotesupport, Dateiübertragung und/oder Remoteaktionen für die Produkte einrichten, die eine oder mehrere dieser Remotezugriffsfunktionen unterstützen.

Hinweis: *Der Policy-Manager kann nur mit der Virtual Edition und den Container Editions des Gateways verwendet werden. Er ist nicht für die Application Edition verfügbar.*

> **Tipps:** Sehen Sie sich eine Vorschau des Policy-Managementmoduls im interaktiven Demo und die technischen Anleitungsvideos für die Virtual Appliance Edition an.

12: Welche Produkte unterstützen die Direktverbindung? Kann ich die Direktverbindung auch mit einem Gateway verwenden?

In einigen Fällen ist unsere Konnektivitätstechnologie in die Betriebsumgebung des Dell Produkts integriert und ermöglicht eine direkte Verbindung zu unserem Services-Backend. Genau das ist mit „Direktverbindung“ gemeint.

Sie werden aufgefordert, die Konnektivitätsservices zu aktivieren, während Sie Ihre Dell Hardware- und Softwareprodukte einrichten.

Sie können Ihr für eine Direktverbindung fähiges Dell Produkt jedoch jederzeit auf eine Verbindung über ein Gateway umstellen. Die Sicherheits- und Netzwerk-Policies Ihres Unternehmens beeinflussen Ihre Konfigurationsentscheidungen.

Dell Infrastrukturprodukte, die eine Direktverbindung unterstützen *Überprüfen Sie immer die neueste Liste der unterstützten Produkte unter Dell.com/Support.*
Appsync | APEX AIOps Infrastructure Observability Collector | CMS – VxBlock-Software
Data Backup/Avamar | Data Domain | Data Domain Management Console | Edge Orchestrator
Elastic Cloud Storage | Metro Node Appliances | ObjectScale
PowerFlex-Produktreihe – Appliance, Rack, Software
PowerProtect – Data Manager, Data Manager Appliance, Scale-out Appliance
PowerScale | PowerStore | PowerVault | S5000-Serie | SRM | Streaming Data | Unity | VxRail
Überprüfen Sie das spezifische Produktmodell und die Version mit Direktverbindungsfunktionen in Ihrer Produktsupportdokumentation.

Hinweis: *Die Softwarefunktionen SupportAssist, SupportAssist Enterprise und Secure Remote Services sind jetzt Teil unserer Konnektivitätssoftwareplattform der nächsten Generation. Die Softwarereferenzen auf der Benutzeroberfläche Ihres Produkts werden im Laufe der Zeit entsprechend aktualisiert.*

13: Was ist das Services-Plug-in für OpenManage Enterprise?

Die secure connect gateway-Technologie wurde auch als Plug-in implementiert. Kunden in einem PowerEdge-Rechenzentrum, die OpenManage nutzen, können jetzt für Warnmeldungen, den automatischen Versand und Erfassungsfunktionen eine Verbindung mit unserem Services-Plug-in für OpenManage Enterprise herstellen.

Ressourcen:

- Weitere Informationen über das Plug-in und Abrufen technischer Ressourcen
- Informationen zu unterstützten Produkten finden Sie in der Supportmatrix zum Produkt auf der Produktsupportseite für OpenManage Enterprise Services.

Erfahren Sie mehr von unseren ExpertInnen:

- **Kurzes Video ansehen** (nur in englischer Sprache)**:** Services-Plug-in für OpenManage Enterprise
- **Podcast anhören** (nur in englischer Sprache)**:** Maximierung der PowerEdge-Verfügbarkeit mit proaktivem, vorausschauendem Support
- **Lesen:** Whitepaper zum Thema Sicherheit

14: Wie erhalte ich Unterstützung bei der Bereitstellung der Konnektivitätssoftware?

Viele Kunden kommen beim Download und bei der Installation unserer Konnektivitätstechnologie ohne Unterstützung von Dell Technologies aus. Sie finden alle erforderlichen Ressourcen auf unserer Webseite.

Tipp: Starten und erkunden Sie unser interaktives technisches Demo.

- *Vorschau der Installation, Registrierung und Verwendung der Gateway Editions und des Policy-Managers*

Für diejenigen, die sich Unterstützung wünschen, umfassen die Services der ProDeploy Infrastructure Suite die Aktivierung und Konfiguration von secure connect gateway.

Kunden mit ProSupport Plus-Abdeckung wird ein/e Service Account Manager (SAM) zugewiesen, der/die bei Fragen zur Installation und Registrierung behilflich sein kann.

Andernfalls können Sie sich bei Bedarf an den Support von Dell Technologies wenden, um Hilfe zu erhalten.

15: Wie kontaktiere ich den Support, wenn Probleme auftreten?

Wenn Sie Probleme mit dem Onlinesupport unter Dell.com oder mit secure connect gateway haben, besuchen Sie hier unsere Seite zum administrativen Support, um Hilfe anzufordern. Wählen Sie die Kategorie aus, die Ihrem Problem am ehesten entspricht, und geben Sie die Details nach Aufforderung ein. Wenn Sie sofortige Unterstützung bei technischen Supportproblemen benötigen, kontaktieren Sie uns hier. Wenden Sie sich an Ihre/n Service Account Manager (falls zutreffend).

Sicherheit

16: Ich möchte mehr über diese Software in der Umgebung des Kunden und die Verbindung zurück zu Dell erfahren. Wie wird diese gesichert?

Die Verbindung zwischen Ihrer Umgebung und Dell wird durch einen gegenseitigen TLS-Tunnel und eine Zertifikatskette gesichert. Bei dieser Art von Konfiguration werden Ihre Systeme mit unserer Software in Ihrer Umgebung verbunden und diese Verbindungen müssen nur interne Port-/Netzwerkänderungen sein. Die Software ist die einzige Komponente, die ausgehende Verbindungen über das Internet und zurück zu Dell herstellt. Sie agiert als Aggregationspunkt für alle Ihre verbundenen Systeme für die Ereignisse und Telemetriedaten. Das sind die einzigen Systemstatusinformationen, die gesendet werden.

Alle Telemetriedaten von den Systemen werden mit HTTPS TLS 1.3 übertragen. Wir stellen außerdem Remotesupportfunktionen über den sicheren Tunnel bereit, um auf Ihr System zuzugreifen und Fehler zu beheben, was die Problemlösung beschleunigt und Ausfallzeiten vermeidet.

Weitere Informationen finden Sie in unserem Whitepaper zum Thema Sicherheit.

17: Wie wird Remotesupport durchgeführt? Wer kann von Dell über eine Remotesupportsitzung auf das System zugreifen?

Bei Dell erstellen die TechnikerInnen des technischen Supports über ein Portal Remotesupportsitzungen, um für das Troubleshooting und für Upgradeaktivitäten auf Ihre Systeme zuzugreifen. Sie verwenden eine Multi-Faktor-Authentifizierung für den Zugriff auf dieses Portal. Diese Dell Teammitglieder müssen strenge Schulungen absolvieren und benötigen eine Freigabe durch das Management, um Zugriff zu erhalten. Wir verwenden das MQTT-Protokoll – eine weithin akzeptierte Lösung für mit Unternehmen verbundene Systeme – als unseren Remotesupport-Agent.

18: Werden diese Systemstatusdaten mit Ereignis- und Telemetrieinformationen angesichts der Fokussierung auf Sicherheit überprüft? Welche Rolle spielt der Policy-Manager?

Wir überprüfen alle Transaktionen und Sie können diese Informationen in der Software auf der Benutzer-oberfläche einsehen. Alle Remotesupportsitzungen, Ereignis- und Telemetrieübertragungen stehen Ihnen zur Verfügung.

Für Kunden mit strengeren Sicherheits-Policies oder für externe AuditorInnen, die eine Speicherung dieser Informationen über einen längeren Zeitraum verlangen, empfehlen wir die Einrichtung unserer Policy-Manager-Software. Unser Policy-Manager arbeitet mit Ihrem secure connect gateway zusammen, um erweiterte Auditing- und Remotesupport-Steuerungsfunktionen bereitzustellen. *Siehe auch Frage 11.*

19: Wo finde ich weitere Informationen zur Sicherheitsarchitektur der Konnektivitäts-technologie?

Laden Sie das Whitepaper zum Thema Sicherheit herunter, um zu erfahren, wie Data Protection und Bedrohungsschutz im secure connect gateway für eine sichere, automatisierte Supporterfahrung integriert sind.

Darin werden folgende Themen behandelt:

- **Sichere Datenerhebung vor Ort:** Erfahren Sie, wie das secure connect gateway als sicherer Kommunikationsbroker agiert, mit dem Kunden u. a. Autorisierungsanforderungen kontrollieren und Protokolle für die Zwei-Faktor-Authentifizierung nutzen können.
- **Sichere Datenübertragung und Kommunikation:** Erfahren Sie, wie das secure connect gateway mithilfe von Verschlüsselung und bilateraler Authentifizierung einen sicheren TLS-Tunnel (Transport Layer Security) für Heartbeat-Abfragen, Remotebenachrichtigungen und Remotezugriffsfunktionen erstellt.
- **Sicherer Daten-Storage sowie sichere Datennutzung und -prozesse:** Hier erfahren Sie mehr über die täglich implementierten Maßnahmen zum Schutz Ihrer Daten, einschließlich physischer Sicherheit, Risikomanagement für Lieferketten und sicherer Entwicklungsprozesse.

Erfahren Sie mehr von unseren ExpertInnen:

- **Podcast anhören** (nur in englischer Sprache)**:** Maximierung der Verfügbarkeit von Rechenzentren mit intelligentem Support
- **Lesen:** Whitepaper zum Thema Sicherheit

Kurze Videos ansehen (nur in englischer Sprache)**:**

- Sicherheitsarchitektur und -funktionen
- Sicherheitskonfiguration für große und kleine Umgebungen
- Sicherheitsfunktionen für den Finanzsektor

Oder sehen Sie sich das Webinar an (nur in englischer Sprache)**:** Erfahren Sie mehr von unseren ExpertInnen in dieser Veranstaltung der Spiceworks-Community, bei der folgende Themen behandelt werden:

- Integration von Datenschutz, Data Protection und Bedrohungsschutz in secure connect gateway
- Flexible Bereitstellung von Konnektivität in kleinen, großen und nicht herkömmlichen Umgebungen
- Warum automatisierter Support dazu beiträgt, Probleme bei verbundenen Systemen zu vermeiden und zu mindern

Konfigurationsszenarien

20: Welche Überlegungen sind bei der Bereitstellung und Konfiguration von Konnektivitätstechnologie für die Anforderungen Ihres Unternehmens zu beachten?

Berücksichtigen Sie zunächst die **Produkttypen – Compute, Storage, Data Protection, konvergente und hyperkonvergente Systeme (CI/HCI) –**, die Sie für die Konnektivität konfigurieren werden, sowie **Ihre aktuelle Umgebung**. Betrachten Sie dabei Folgendes:

- Sind Ihre Rechenzentren miteinander vernetzt oder nicht?
- Managen Sie Compute oder Storage (einschließlich Data Protection, CI-/HCI-Produkte) *separat oder gemeinsam*?

Sie müssen außerdem die **Sicherheits- und Netzwerk-Policies** des Unternehmens berücksichtigen und bedenken, **ob Ihre Teams alle Produkte gemeinsam verwalten oder sie lieber nach geografischem Standort oder Produkttyp segmentieren möchten**.

Im Wesentlichen müssen Sie darüber nachdenken, wie Systeme verbunden sind, wie Teams zusammenarbeiten und wie Sie die Netzwerkkomplexität minimieren können. Auf diese Weise können Sie die effektivste Architektur basierend auf den verschiedenen Bereitstellungsoptionen entwerfen.

Lesen und teilen Sie unsere Übersicht zu Überlegungen zur Konnektivitätskonfiguration, die Folgendes abdeckt:

1. Was ist die empfohlene Konfiguration für ein größeres sicherheitsbewusstes Unternehmen?
2. Welche Konfigurations- und Bereitstellungsoptionen gibt es für ein mittleres bis kleines Unternehmen?
3. Was ist, wenn ich ein großes bis mittelgroßes Unternehmen mit einer Compute-zentrierten Umgebung bin? Wie entscheide ich, welches Tool ich verwende?
4. Was passiert, wenn ich rund 1 bis 50 PowerEdge-Server und keine virtualisierte Umgebung habe? Welche Gatewayoptionen stehen mir zur Verfügung?
5. Was geschieht, wenn ich Dell Produkte mit Direktverbindungsverfügbarkeit habe? Was sind typische Anwendungsfälle?
6. Welche ist die richtige Konfiguration für mein Unternehmen?

Support Services

21: Inwiefern ist die Konnektivität für den Mehrwert des Supportservicevertrags für meine Dell Infrastrukturprodukte relevant?

Kurz gesagt: Sie können einen Mehrwert aus Ihren aktiven Supportverträgen für Dell Systeme ziehen, indem Sie unsere Konnektivitätssoftware in Ihrer Umgebung bereitstellen und Ihre Dell Geräte verbinden, die von dieser Software überwacht werden sollen. Es handelt sich um kostenlose Software – es ist keine Lizenz erforderlich. Wir unterstützen über 90 Dell Infrastrukturprodukte – Hardware und Software. Sie profitieren von unserer einzigartigen Integration von intelligenterer KI, automatisiertem Support und Echtzeitanalysen.

Kunden mit ProSupport Infrastructure Suite-Services erhalten auf allen Ebenen einen hohen Mehrwert.

- Weitere Informationen: ProSupport- und ProSupport Plus-Abdeckung für Dell Infrastruktursysteme
    - Weitere Informationen: Lifecycle Extension with ProSupport oder ProSupport Plus
- Hinweis: Dell Systeme mit Basic Hardware Support (Next Business Day) profitieren ebenfalls von unseren proaktiven, automatisierten Funktionen zur Problemerkennung, Fallerstellung und Benachrichtigung, wenn sie von unserer Konnektivitätssoftware überwacht werden. Wenn ein Problem festgestellt wird, erhalten Basic Support-Kunden eine E-Mail mit der Fallnummer und werden aufgefordert, sich zeitnah mit dem Dell Support in Verbindung zu setzen, um zu bestätigen, dass sie Unterstützung von Dell beim Troubleshooting und bei der Lösung wünschen.

Erkunden Sie außerdem unsere spezialisierten Support Services für Infrastruktur

22: Was geschieht mit den automatisierten Supportfunktionen, wenn die Abdeckung des Supportservicevertrags, z. B. mit ProSupport Infrastructure Suite, auf meinem überwachten System abläuft?

Wenn Ihr Servicevertrag für ein beliebiges Level der ProSupport Infrastructure Suite ausläuft, wird die Funktion zur automatischen Fallerstellung deaktiviert. Die als Gateway, Direktverbindung oder Plug-in bereitgestellte secure connect gateway-Technologie führt jedoch weiterhin automatisierte Datenerfassungen zum Systemstatus aus. Wenn Sie den Vertrag für ein System (Service-Tag) aktualisieren oder verlängern, wird die Funktion zur automatischen Fallerstellung auf diesem System automatisch wieder aktiviert.

Konnektivität für PowerEdge

23: Wie lässt sich diese Konnektivitätssoftware für Server am besten bereitstellen und konfigurieren? Wie entscheiden Sie, welches Tool verwendet werden soll?

Kurz gesagt: Das Services-Plug-in über die OpenManage Enterprise-Lösung eignet sich gut für Kunden mit Compute-zentrierten Umgebungen, während die Gatewaylösung die ideale Wahl für das Management einer Vielzahl von Dell Infrastrukturprodukten ist.

Beide Lösungen umfassen unsere Funktionen für Warnmeldungen, automatische Fallerstellung, automatischen Versand und Telemetrieerfassung für PowerEdge-Server mit einem Supportvertrag.

Was Sie auswählen, hängt von der Art Ihrer Umgebungen, den Netzwerken zwischen diesen Umgebungen, den überwachten Gerätetypen und Ihren Präferenzen ab.

Wenn Sie OpenManage Enterprise eingerichtet haben oder dies planen, ist das Services-Plug-in die richtige Option für Sie. OpenManage Enterprise ist die Infrastrukturlösung von Dell, die das Lebenszyklusmanagement von Tausenden von PowerEdge-Servern über eine einzige Konsole ermöglicht.

- Wenn Sie damit noch nicht vertraut sind, installieren Sie einfach Open Manage Enterprise in Ihrer Umgebung, integrieren Sie Ihre Serverprodukte und installieren Sie dann unser Services-Plug-in. Stellen Sie sicher, dass Ihre Firewall korrekt konfiguriert ist, damit Warnmeldungen und Telemetriedaten an Dell zurückgesendet werden.

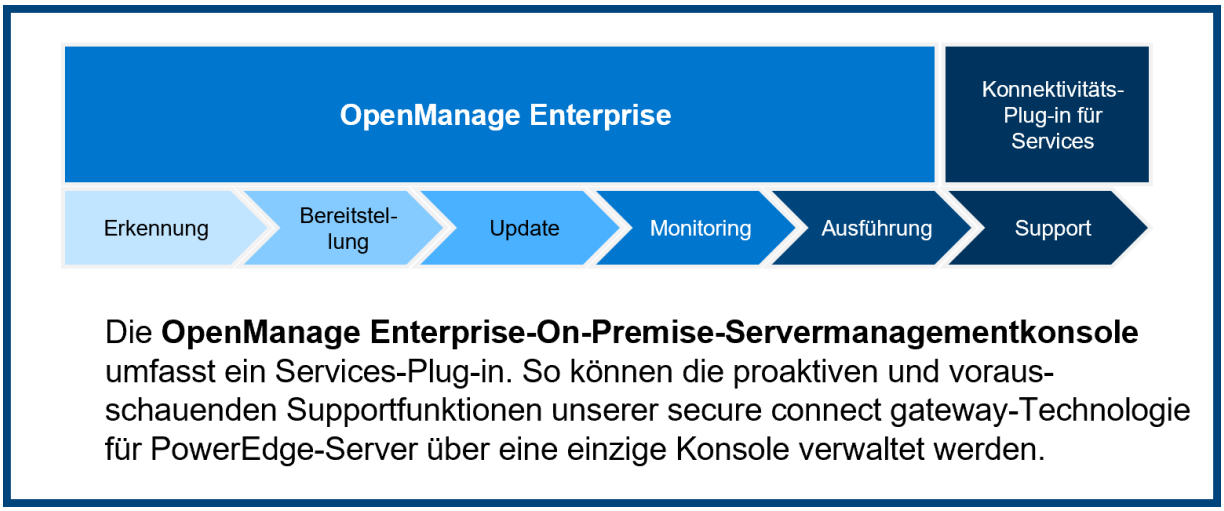
Kunden mit einer Mischung aus Dell Infrastrukturprodukten wie PowerStore, PowerMax, PowerScale, Data Domain und VxRail, die zusammen mit PowerEdge ausgeführt werden, empfehlen wir, unsere secure connect gateway-Lösung einzurichten, um diese Systeme über eine einzige Benutzeroberfläche zu verwalten.

Erfahren Sie mehr von unseren ExpertInnen:

- **Podcast anhören** (nur in englischer Sprache)**:** Maximierung der PowerEdge-Verfügbarkeit mit proaktivem, vorausschauendem Support
    - Erforderliche Schritte für die Verbindung von PowerEdge-Systemen über die OpenManage Enterprise-Lösung und Vergleich zu einer Verbindung über eine Gatewaylösung
    - Anleitung zum Herstellen einer Verbindung mit den PowerEdge-Geräten selbst
    - Anleitung zur einfachen Skalierung der Anzahl verbundener Server über die Zeit
    - Andere Konfigurationsszenarien: Ausführung der Plug-in- und Gatewayoptionen

24: Inwiefern ergänzt die Konnektivität für Services das Lebenszyklusmonitoring des Rechenzentrumsmanagements von OpenManage Enterprise?

OpenManage Enterprise ist eine benutzerfreundliche 1:n-Systemmanagementkonsole, mit der das umfassende Lebenszyklusmanagement für PowerEdge-Server und -Gehäuse auf kosteneffiziente Weise in einer einzigen Konsole vereinfacht wird. Das Diagramm unten zeigt, wie das Konnektivitäts-Plug-in für OpenManage Enterprise die OpenManage Enterprise-Erfahrung für das Rechenzentrum ergänzt. Diese Funktion ist derzeit über das Services-Plug-in für OpenManage Enterprise verfügbar. Weitere Informationen und Ressourcen finden Sie hier.



25: Welche Systeme werden vom Services-Plug-in für OpenManage Enterprise unterstützt?

PowerEdge-Server und Gehäuse mit iDRAC und Chassis Management Controller (CMC) sowie Linux-Server werden unterstützt.

Um die spezifischen unterstützten Produkte zu überprüfen, besuchen Sie die Website Dell.com/Support und sehen Sie sich das Supportmatrix-Dokument auf der Produktsupportseite für OpenManage Enterprise Services an.

Veröffentlicht in Deutschland. 7/24

Weitere allgemeine Highlights

26: Wo finde ich Informationen zu den Warnmeldungs-Policies für secure connect gateway? Wann werden vorausschauende Supportfälle für Hardwareausfälle erstellt?

Unsere Policy für Secure Connect Gateway-Warnmeldungen enthält Informationen zu den Warnmeldungen, durch die Fälle beim technischen Support von Dell Technologies erstellt werden. Kunden, die das secure connect gateway verwenden, können die automatisierte vorausschauende Fallerstellung für Serverhardware (Festplatte, Rückwandplatine und Expander) nur auf Systemen mit einem ProSupport Plus-Servicevertrag in Anspruch nehmen. Vorausschauende Warnmeldungen basieren auf geplanten Erfassungen von Systemdaten, die an Dell Technologies gesendet werden.

27: Was muss ich über die Funktionen für das Zugangsdatenmanagement des Gateways wissen?

Das secure connect gateway bietet die Flexibilität, mehrere Zugangsdatenkonten und Profile hinzuzufügen. Mithilfe der Zugangsdatenkonten können AdministratorInnen Authentifizierungen nach Produkttyp hinzufügen. Außerdem können mithilfe von Profilen mehrere AdministratorInnen, die sich nach Funktion oder Region unterscheiden, für das Management spezifischer Konten festgelegt werden. Zu den Produkten, für die Zugangsdaten benötigt werden, zählen PowerEdge-Server, iDRAC, Compellent, Netzwerke, PS Series, MD-Serie und Webscale-Systeme.

Wir bieten auch die Integration von Zugangsdaten-Vaults an. Dies ist eine großartige Funktion für Kunden mit vielen Geräten, da sie Systeme hinzufügen und die richtigen Zugangsdaten verwalten können, ohne die Sicherheit zu gefährden oder den manuellen Aufwand zu erhöhen. CyberArk Conjur-APIs und CyberArk Credential Provider-Produkte werden derzeit unterstützt. Weitere Anbieter werden hinzugefügt. Die aktuelle Liste finden Sie in unserer Supportdokumentation.

Tipp: Eine Vorschau dieser Funktionen finden Sie im Modul *Gerätemanagement* im interaktiven Demo**.**

28: Was sind die wichtigsten Funktionen des Wartungsmodus?

Ein „Ereignissturm“ tritt auf, wenn schnell hintereinander Hardwarewarnmeldungen erfolgen, deren Anzahl einen vordefinierten Grenzwert überschreitet. In diesem Szenario beendet das secure connect gateway die Verarbeitung von Warnmeldungen für diejenigen Geräte, die den Ereignissturm ausgelöst haben. Alle anderen Geräte werden weiterhin vom secure connect gateway auf validierte Warnmeldungen überwacht, für die ggf. Supportanfragen erstellt werden.

Außerdem haben NutzerInnen jetzt die Möglichkeit, die Wartung auf einem oder mehreren Geräten manuell im System zu aktivieren. Diese Option kann für die geplante Wartung verwendet werden und wird bereitgestellt, wenn Sie nicht möchten, dass das secure connect gateway diese Geräte überwacht. Sobald die geplanten Wartungsaktivitäten abgeschlossen sind, können Sie den Wartungsmodus manuell deaktivieren, um dem secure connect gateway zu signalisieren, das Monitoring wieder aufzunehmen.

29: Kann ich mit der Gatewayoption Einstellungen für E-Mail-Benachrichtigungen festlegen?

Ja. Ihre Einstellungen für E-Mail-Benachrichtigungen können über die secure connect gateway-Benutzer-oberfläche auf der Registerkarte für Einstellungen angepasst werden. Weitere Informationen finden Sie im Benutzerhandbuch.

30: Welche Sprachen werden im Managementdashboard des On-Premise-Gateways unterstützt?

Die secure connect gateway-Softwarebenutzeroberfläche steht in Englisch, Deutsch, brasilianischem Portugiesisch, Französisch, Spanisch, vereinfachtem Chinesisch und Japanisch zur Verfügung. Kunden können jedoch eine von 28 Sprachen für automatische E-Mail-Benachrichtigungen auswählen, die zum Zeitpunkt eines Service-Request-Incidents gesendet werden. Hinweis: Einige E-Mail-Benachrichtigungen werden aufgrund von Einschränkungen des Betriebssystems nicht in die Landessprache übersetzt.

31: Wie nutze ich REST APIs?

Mit der Gatewayoption können Kunden ihr eigenes kundenspezifisches Scripting mit REST APIs durchführen und unterstützen. Laden Sie das Benutzerhandbuch für REST APIs aus unserem Dokumentationsbereich herunter.

32: Wie wird diese Konnektivitätssoftware für APEX AIOps Infrastructure Observability (ehemals CloudIQ) verwendet?

APEX AIOps Infrastructure Observability (ehemals CloudIQ) trägt dazu bei, die Integrität der Core-, Edge- und Multi-Cloud-Infrastruktur von Dell durch KI-gesteuerte Erkenntnisse und Empfehlungen in den Bereichen Integrität, Cybersicherheit und Nachhaltigkeit zu optimieren.

- Zu den wichtigsten Attributen gehören: Bewertungen des Integritätsstatus und der Cybersicherheitsrisiken sowie Empfehlungen für Korrekturen, Nachverfolgung der Performance und Kapazität, Anomalieerkennung und Prognosen, Vorhersage von Fehlern, Nachverfolgung und Prognose von Energieverbrauch und Emissionen sowie Überwachung von Virtualisierungsressourcen.

Unsere Konnektivitätssoftware wird ausschließlich für die Übertragung von System- und Ereignisdaten aus der Kundenumgebung verwendet. Die Telemetriedaten werden sicher zurück an das Dell Backend übertragen und dort von den KI-Algorithmen für APEX AIOPs Infrastructure Observability analysiert.

Funktionshighlight (ohne Bezug zu Konnektivität):

- Im Infrastructure Observability-Portal steht auch der AIOps Assistant zur Verfügung, der generative KI nutzt, um sofortige, detaillierte Antworten und Empfehlungen zur Problemlösung für die Dell Infrastruktur bereitzustellen.