Konnektivität für Unternehmenssysteme

Inhaltsverzeichnis

14. Was muss ich über die Funktionen für das Zugangsdatenmanagement des sicheren Verbindungsgateways wissen?
15. Was sind die wichtigsten Funktionen des Wartungsmodus?
16. Welche Optionen kann ich nutzen, wenn ich nur 1–3 Server habe und weder das sichere Verbindungsgateway noch das Services-Plug-in für OpenManage Enterprise installieren möchte?

Allgemeine Funktionshighlights – Fortsetzung

17. Was geschieht mit Funktionen des sicheren Verbindungsgateways, wenn mein überwachtes System nicht mehr durch ProSupport Enterprise Suite oder ProSupport One for Data Center abgedeckt ist?
18. Kann ich im sicheren Verbindungsgateway Einstellungen für E-Mail-Benachrichtigungen festlegen?
19. Welche Sprachen werden im Dashboard für das On-Premise-Konnektivitätsmanagement im sicheren Verbindungsgateway unterstützt?
20. Wo kann ich Versandbenachrichtigungen anzeigen, wenn meine Geräte angeschlossen sind?
21. Welche Produkte haben Remotezugriffsfunktionen, die vom sicheren Verbindungsgateway verwaltet werden?
22. Was ist der Policy Manager für das sichere Verbindungsgateway?
23. Wie nutze ich REST APIs?

Funktionshighlights: OpenManage Enterprise-Umgebung für PowerEdge-Server

24. Welche Systeme werden vom Konnektivitäts-Plug-in für OpenManage Enterprise unterstützt?
25. Welche Voraussetzungen gelten für das Monitoring der Konnektivität von PowerEdge-Geräten?
26. Inwiefern ergänzt die Konnektivität für Services das Lebenszyklusmonitoring des Rechenzentrums-managements von OpenManage Enterprise?

Sicherheitsinformationen

27. Wo finde ich weitere Informationen zur Sicherheitsarchitektur der Konnektivitätstechnologie?

Allgemeine Informationen

1. **Was beinhaltet die Sicheres Verbindungsgateway 5.x-Technologie? Ersetzt sie die SupportAssist Enterprise- und Secure Remote Services-Lösungen?**

   Die Sicheres Verbindungsgateway 5.x-Technologie steht für die konsolidierte Konnektivitätslösung der nächsten Generation von Dell Technologies Services. Sie ersetzt die Legacy-Lösungen SupportAssist Enterprise und Secure Remote Services, deren Funktionen in die Technologie für das sichere Verbindungsgateway integriert sind.

   Unsere Sicheres Verbindungsgateway 5.x-Technologie ist eine Remote-IT-Support- und -Monitoringsoftware, die als Appliance und als eigenständige Anwendung bereitgestellt wird. Sie bietet eine einzige Lösung für das gesamte Dell Portfolio, die Server, Netzwerke, Daten-Storage, Data Protection sowie hyperkonvergente und konvergente Lösungen unterstützt. Darüber hinaus bietet diese Version Folgendes:

   - Einblick in die kritischsten Probleme
   - Beschleunigte Problembehebung durch Remotezugriff und sichere bidirektionale Kommunikation zwischen Dell Technologies und der Kundenumgebung
   - Eine Installation und Registrierung für das Rechenzentrum
   - Empfehlung zum Herunterladen und Installieren von VMware Skyline Collector, wenn SupportAssist vCenter in der Umgebung identifiziert
     - Dies wird nur für Kunden empfohlen, die Skyline nicht installiert haben. Skyline Collector wird nur Kunden mit Anspruch auf VMware Premier oder Production angeboten.
   - Fortlaufender Fokus auf Sicherheit mit einem neuen Policy Manager 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

   Diese Technologie steht neuen und aktuellen Dell Technologies Konnektivitätskunden mit Service oder einem Servicelevel-Vertrag für ProSupport Enterprise Suite zur Verfügung.

   Aktuelle Kunden, die unsere Legacy-Konnektivitätsplattformen Secure Remote Services 3.x sowie SupportAssist Enterprise v4.x und v2.x nutzen, können ein einfaches Upgrade auf unsere neueste Technologie – Sicheres Verbindungsgateway – mit minimaler Unterbrechung durchführen.

   Kunden wird dringend empfohlen, ihre Unternehmenskonnektivität proaktiv zu aktualisieren, um Unterbrechungen beim automatisierten, intelligenten Support für Systeme zu vermeiden.
   In Frage 3 finden Sie Details zum Ende der Nutzungsdauer für Legacy-Lösungen und in Frage 6 Ratschläge zu Upgrades.

2. Gibt es neben der Verwendung des sicheren Verbindungsgateways noch andere Möglichkeiten, eine Verbindung herzustellen?

Ja. Kunden in einem PowerEdge-Rechenzentrum, die OpenManage nutzen, können jetzt für Warn-, Auto-Dispatch- und Erfassungsfunktionen eine Verbindung mit unserem Services-Plug-in für OpenManage Enterprise herstellen.

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.

3. Kann ich die SupportAssist Enterprise- und Secure Remote Services-Technologie weiterhin verwenden? Wann werden diese Lösungen eingestellt?

Wenn Sie Neuling in Supporttechnologien sind, sollten Sie diese älteren Technologien nicht herunterladen und verwenden.

Zusammenfassung der Legacy-Technologielösungen

SupportAssist Enterprise 4.x	**SupportAssist Enterprise v2.x**	**Secure Remote Services (SRS) Version 3.x** (früher ESRS)
Für Server-, Storage-, Netzwerk- und CI-/HCI-Geräte; wird als eigenständige Anwendung oder mit der führenden Managementkonsole OpenManage Enterprise bereitgestellt	Für Server-, Storage- und Netzwerkgeräte; wird als eigenständige Anwendung oder mit den führenden Managementkonsolen OpenManage Essentials, OpenManage Enterprise oder Microsoft System Center Operations Manager (SCOM) bereitgestellt; kein direkter Upgradepfad von SupportAssist Enterprise 2.x auf 4.x	Für Storage-, Data-Protection- und CI-/HCI-Produkte; wird als virtuelle Appliance oder containerisiertes System bereitgestellt; kein direkter Upgradepfad von Secure Remote Services auf SupportAssist Enterprise 4.x

Wirksamkeitsdaten für das Ende der Nutzungsdauer (EOSL) für Legacy-Lösungen:

- **SupportAssist Enterprise 2.x und 4.x** werden am 31. Juli 2022 eingestellt.
- **Secure Remote Services 3.x** wird für alle Dell Produkte am 15. Juni 2023 eingestellt, mit zwei Ausnahmen: Für Kunden mit PowerStore- und Unity-Produkten, die Direct Connect nutzen, werden wir Secure Remote Services 3.x im Juni 2024 einstellen.

Am Wirksamkeitsdatum erreichen alle Versionen der angegebenen Konnektivitätslösung das Ende ihrer Nutzungsdauer (EOSL). Infolgedessen wird der Support (einschließlich Korrektur und Minderung von Sicherheitslücken) für die Lösung eingestellt. Die Ersatzlösung ist das neue sichere Verbindungsgateway.

- *Hinweis: Die proaktiven und vorausschauenden Funktionen der Legacy-Konnektivität für Dell Produkte werden eingestellt, es sei denn, das Upgrade auf die Ersatztechnologie ist vorhanden.*

Wenn sich das Datum des Endes der Nutzungsdauer nähert, sendet Dell Technologies Services eine Benachrichtigungs-E-Mail an betroffene Kunden, in der das Ende des Supports und der Wartung bekannt gegeben wird.

Für alle, die Secure Remote Services 3.x sowie SupportAssist Enterprise v4.x und v2.x verwenden:

Direkte Upgradepfade erleichtern die Einführung der Sicheres Verbindungsgateway 5.x-Technologie mit minimaler Unterbrechung. Beginnen Sie mit den Upgradelinks im Gatewaymanagement-dashboard.

Ressourcen: Interaktives Demo | Technische Videos – Application Edition | Virtual Appliance Edition

4. **Welche Bereitstellungsoption für das sichere Verbindungsgateway eignet sich am besten für meine Umgebung?**

Wählen Sie anhand der Tabelle die geeignete Option für Ihre Umgebung aus. Sehen Sie in der Produktsupportmatrix für das sichere Verbindungsgateway 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 unterstützte Hardware und Software (siehe unten) verwenden.

Verbindung über Gatewaytechnologie zur Überwachung aller Geräte an einem Ort

Integrierte Gatewaylösungen	Unterstützte Hardware und Software*
Sicheres Verbindungsgateway 5.x – Virtual Appliance Edition *Für VMware* *Für Microsoft Hyper-V*	Gesamtes Dell EMC Produktportfolio – Daten-Storage, Server, Netzwerke, CI/HCI und Data Protection
Sicheres Verbindungsgateway 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
* Hinweis: Unsere Technologie unterstützt die Konnektivität mit VMware Skyline für PowerEdge-Server, auf denen vCenter ausgeführt wird.	

Direkte Verbindung für ausgewählte Dell EMC Hardware

- Integration von Konnektivität in die Betriebsumgebung von Dell EMC Produkten
- Geeignet für die heterogene Bereitstellung von mehreren Dell EMC Hardwareprodukten
- Direkte Verbindung zu Dell Technologies oder über den Server für das sichere Verbindungsgateway

5. **Welche Software wird für meine Umgebung empfohlen und welche Mindestanforderungen gelten?**

   Sicheres Verbindungsgateway – Virtual Edition:
   Es gibt Versionen für:
   - VMware-Umgebungen
   - Microsoft Hyper-V-Umgebungen

   Überprüfen Sie die Mindestanforderungen, die für die Installation und Nutzung der Software für das sichere Verbindungsgateway gelten.Laden Sie die Dokumentation und alle Ressourcen von Dell.com/Support herunter.

   Sicheres Verbindungsgateway – Application Edition:
   Es gibt Versionen für:
   - Windows-Managementserver (überwacht sowohl Windows- als auch Linux-Geräte)
   - Linux-Managementserver (überwacht Linux-Geräte)

   Überprüfen Sie die Mindestanforderungen für die Installation und Verwendung der Software.Laden Sie die Dokumentation und alle Ressourcen von Dell.com/Support herunter.

   Tipps für neue Nutzer beim Einstieg:

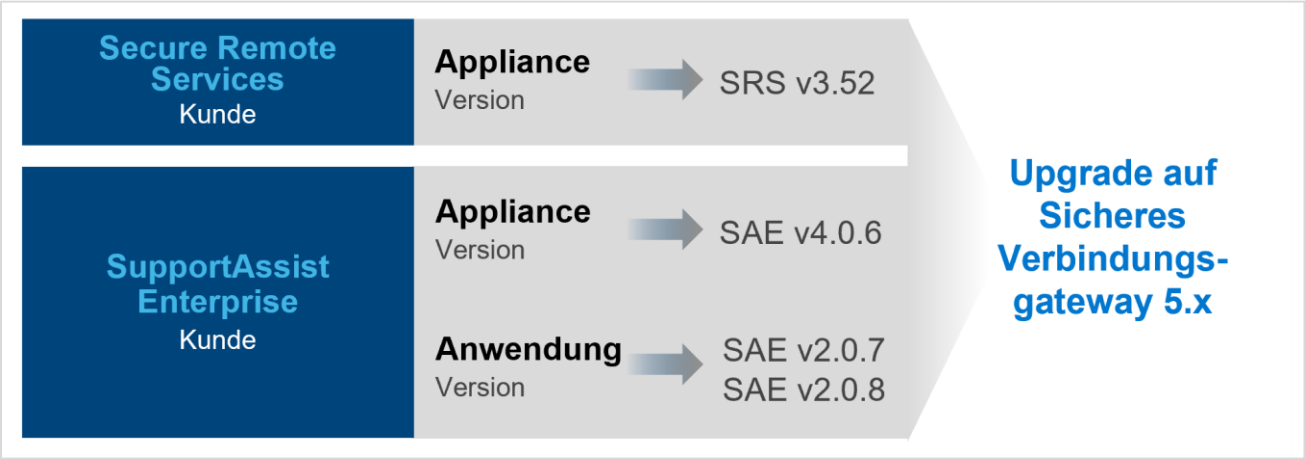
   - Neue NutzerInnen müssen zuerst ein Enterprise-Geschäftskonto auf Dell.com/Support einrichten. Sie werden auf der Downloadseite zum sicheren Verbindungsgateway aufgefordert, sich anzumelden und diesen Schritt abzuschließen.
   - Melden Sie sich danach mit Ihren Kontozugangsdaten bei der Produktsupportseite für Sicheres Verbindungsgateway auf Dell.com/Support an.
   - Stellen Sie sicher, dass Sie den Standort der Softwareinstallation 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.

   Erkunden der Technologie: Starten Sie unser interaktives technisches Demo.
   - *Das Demo deckt Neuinstallationen der Application und Virtual Appliance Edition, die Einrichtung von Enterprise-Unternehmenskonten (enthalten in den Modulen 1 und 2), Upgrades von Legacy-Lösungen, die Funktionen des Gatewaymanagementdashboards und den Policy Manager (nur Virtual Edition) ab.*

   Benötigen Sie Hilfe? Stellen Sie unseren ExpertInnen beliebige Fragen über das Forum für das sichere Verbindungsgateway.

6. **Welche Version von SupportAssist Enterprise oder Secure Remote Services sollte auf meinem System ausgeführt werden, damit ich ein Upgrade auf Sicheres Verbindungsgateway 5.x durchführen kann?**

   Sie müssen sicherstellen, dass für Ihre Dell Hardware oder Software die folgenden Versionen von SupportAssist Enterprise oder Secure Remote Services ausgeführt werden. Sie werden auf Ihrer Webbenutzeroberfläche zum Upgrade auf die Sicheres Verbindungsgateway 5.x-Technologie aufgefordert.



   Tipp: Eine Vorschau der Schritte finden Sie in Modul 3, *Upgrade von Secure Remote Services 3.52*, und Modul 4, *Upgrade von SupportAssist Enterprise 2.0.7 und 2.0.8*, im interaktiven Demo.

7. **Welche automatisierten Supportfunktionen sind bei ProSupport Enterprise Suite-Abdeckung verfügbar?**

Funktionen	Basic	ProSupport	ProSupport Plus
Automatisierte Problemerkennung und Erfassung von Systemstatusinformationen	●	●	●
Proaktive, automatisierte Fallerstellung und Versandbenachrichtigung		●	●
Vorausschauende Problemerkennung zur Vermeidung von Ausfällen[1]			●

1. Vorausschauende Analysen zur Fehlerbehebung umfassen Serverfestplatten und -rückwandplatinen, wenn sie über das sichere Verbindungsgateway verbunden sind.

   Erfahren Sie mehr über Enterprise Support Services für die Einbeziehung von ProSupport Enterprise Suite-Services.

8. **Wie kann ich mit der Technologie für das sichere Verbindungsgateway Zeit beim Troubleshooting sparen?**

   Unsere Konnektivitätstechnologie erkennt automatisch Probleme, erfasst Systemstatusinformationen und initiiert Warnmeldungen und den Kontakt zu Dell Technologies. Sie sparen die Zeit, die Sie sonst für die Erfassung von Systemstatusinformationen, die Fallerstellung und die Kontaktaufnahme mit Dell Technologies aufwenden. Mit dem sicheren Verbindungsgateway können Sie Systemstatus-informationen auch automatisch oder bedarfsorientiert erfassen und automatisch an Dell versenden, um proaktiv einen Fall erstellen zu lassen. Je nach Problem und Ihren Einstellungen kann das Gateway eine Remotelösung mittels Remotezugriff über eine sichere bidirektionale Kommunikation zwischen Ihnen und Dell Technologies initiieren.

9. **Muss ich mein Gerät mit Sicheres Verbindungsgateway 5.x bei Dell Technologies registrieren?**

   Ja. Um das sichere Verbindungsgateway zu verwenden und erstklassige Sicherheit zu erzielen, müssen Sie sich bei Dell Technologies registrieren. Melden Sie sich mit Ihrem Enterprise-Unternehmenskonto auf der Downloadseite an, generieren Sie einen Zugriffsschlüssel und eine PIN und verwenden Sie beides, um Ihr sicheres Verbindungsgateway zu aktivieren. Kunden, die kein Unternehmenskonto haben, werden aufgefordert, zusätzliche Informationen über ihr Unternehmen und ihre Produkte anzugeben. Nach der Verifizierung kann der Kunde fortfahren.

10. **Wie erhalte ich Unterstützung, um Technologie für das sichere Verbindungsgateway bereitzustellen?**

    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.

    - *Das Demo deckt Neuinstallationen der Application und Virtual Appliance Edition, die Einrichtung von Enterprise-Unternehmenskonten (enthalten in den Modulen 1 und 2), Upgrades von Legacy-Lösungen, die Funktionen des Gatewaymanagementdashboards und den Policy Manager (nur Virtual Edition) ab.*

    Für alle, die Unterstützung benötigen, beinhaltet die ProDeploy Enterprise Suite von Services die Aktivierung und Konfiguration des sicheren Verbindungsgateways. Kunden mit ProSupport Plus-Abdeckung wird ein Service Account Manager (SAM) zugewiesen, der bei Installations- und Registrierungsfragen behilflich ist. Wenden Sie sich andernfalls an den Dell Technologies Support, um Unterstützung zu erhalten.

11. **Wie kontaktiere ich den Support, wenn Probleme auftreten?**

    Wenn Sie Probleme mit dem Onlinesupport auf Dell.com oder dem sicheren Verbindungsgateway 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 Ihren Service Account Manager (falls zutreffend).

Allgemeine Funktionshighlights

12. Wo finde ich Informationen zu den Warnmeldungs-Policies für das sichere Verbindungs-gateway? Wann werden vorausschauende Supportanfragen für Hardwareausfälle erstellt?

Unsere Policy für Warnmeldungen zum sicheren Verbindungsgateway enthält Informationen zu den Warnmeldungen, durch die Fälle beim technischen Support von Dell Technologies erstellt werden. Kunden, die das sichere Verbindungsgateway 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.

13. Wie kann ich automatisierte Warnmeldungsdaten von Dell in meinem Dashboard unter *Connect and Manage* im TechDirect-Portal anzeigen?

Im TechDirect-Onlinedashboard können Sie auf der Registerkarte *Connect and Manage* Warnmeldungen und Ressourcen für Ihr Unternehmen verwalten. Hier können IT-Administrator-Innen Regeln festlegen, um automatisierte Warnmeldungen für die Erstellung von Supportanfragen oder den Ersatzteilversand zu überprüfen und zu bestimmen, ob sie an Dell Technologies weiterzuleiten sind.

Wichtige Konnektivitätsanforderung für Daten: Der Kunde muss Warnmeldungsdaten im Rahmen der Konfiguration des On-Premise-Gateways in dieses Dashboard integrieren. Dies gilt für Gatewayeditionen und das Plug-in für die OpenManage Enterprise-Umgebung.

Hinweis: Diese Funktion ist für PowerEdge, iDRAC, PowerSwitch, Webscale, PeerStorage, EqualLogic, Compellent, Fluid File System (FluidFS), PowerVault- und PowerStore-Systeme verfügbar, die SupportAssist Enterprise 2.x, OpenManage Enterprise SupportAssist Plug-in 1.x, OpenManage Enterprise Services Plug-in 1.x, SupportAssist Enterprise 4.x und/oder Sicheres Verbindungsgateway 5.x verwenden. Vergessen Sie nicht, die erforderlichen Integrationsschritte im Benutzer- oder Installationshandbuch des Produkts nachzulesen.

Sonstiges: Warnmeldungen von Geräten, die mit Secure Remote Services-Technologie verbunden sind, werden im TechDirect-Dashboard *Enterprise Assets and Alerts* nicht unterstützt.

14. Was muss ich über die Funktionen für das Zugangsdatenmanagement des sicheren Verbindungsgateways wissen?

Das sichere Verbindungsgateway 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 Accounts festgelegt werden. Zu den Produkten, für die Zugangsdaten benötigt werden, zählen PowerEdge-Server, iDRAC, Compellent, Netzwerke, PS Serie, MD Serie und Webscale-Systeme.

Tipp: Eine Vorschau dieser Funktionen finden Sie im Modul *M5.3 Gerätemanagement*im interaktiven Demo.

15. Was sind die wichtigsten Funktionen des Wartungsmodus?

Ein „Ereignissturm“ tritt auf, wenn schnell hintereinander Hardwarewarnmeldungen erfolgen, deren Anzahl einen vordefinierten Grenzwert überschreiten. In diesem Szenario beendet das sichere Verbindungsgateway die Verarbeitung von Warnmeldungen für diejenigen Geräte, die den Ereignissturm ausgelöst haben. Alle anderen Geräte werden weiterhin vom sicheren Verbindungsgateway 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 sichere Verbindungsgateway diese Geräte überwacht. Sobald die geplanten Wartungsaktivitäten abgeschlossen sind, können Sie den Wartungsmodus manuell deaktivieren, um dem sicheren Verbindungsgateway zu signalisieren, das Monitoring wieder aufzunehmen.

16. Welche Optionen kann ich nutzen, wenn ich nur 1–3 Server habe und weder das sichere Verbindungsgateway noch das Services-Plug-in für OpenManage Enterprise installieren möchte?

Für Kunden mit PowerEdge-Servern der 14. und 15. Generation wird die Konnektivität auf Basis der SupportAssist-Technologie werkseitig in den Server integriert. Um automatischen proaktiven und vorausschauenden Support zu erhalten, aktivieren Sie das iDRAC-Servicemodul (iSM) und registrieren SupportAssist in der iDRAC-Konsole.

17. Was geschieht mit Funktionen des sicheren Verbindungsgateways, wenn mein überwachtes System nicht mehr durch ProSupport Enterprise Suite oder ProSupport One for Data Center abgedeckt ist?

Wenn Ihr Servicevertrag für ProSupport Enterprise Suite oder ProSupport One for Data Center ausläuft, wird die Funktion zur automatischen Fallerstellung deaktiviert. Daten zum Systemstatus werden jedoch weiterhin automatisch vom sicheren Verbindungsgateway erfasst. Wenn Sie den Vertrag für ein System (Service-Tag) aktualisieren oder verlängern, wird die Funktion zur automatischen Fallerstellung auf diesem System automatisch wieder aktiviert.

18. Kann ich im sicheren Verbindungsgateway Einstellungen für E-Mail-Benachrichtigungen festlegen?

Ja. Ihre Einstellungen für E-Mail-Benachrichtigungen können über die Benutzeroberfläche des sicheren Verbindungsgateways auf der Registerkarte für Einstellungen angepasst werden. Weitere Informationen finden Sie im Benutzerhandbuch.

19. Welche Sprachen werden im Dashboard für das On-Premise-Konnektivitätsmanagement im sicheren Verbindungsgateway unterstützt?

Die Softwareschnittstelle des sicheren Verbindungsgateways steht in Englisch, Deutsch, brasilianischem Portugiesisch, Französisch, Spanisch, vereinfachtem Chinesisch und Japanisch zur Verfügung. Kunden können jedoch eine (1) 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.

20. Wo kann ich Versandbenachrichtigungen anzeigen, wenn meine Geräte angeschlossen sind?

Im TechDirect-Portal über das Dashboard *Connect and Manage* zur Verwaltung von Unternehmensressourcen und -warnmeldungen:

- Hier können Sie Ihre Versandpräferenzen für berechtigte Dell Server, Netzwerke und Storage-Systeme überprüfen.
- Wichtige Konnektivitätsanforderung für Daten: Der Kunde muss Warnmeldungsdaten im Rahmen der Konfiguration des On-Premise-Gateways in dieses Dashboard integrieren. Dies gilt für Gatewayeditionen und das Plug-in für die OpenManage Enterprise-Umgebung. Lesen Sie Frage 13 in diesem Dokument.

Im Analysedashboard im MyService360-Portal:

- Hier können Sie die Versandbenachrichtigungen für berechtigte Dell Storage-, Data-Protection- und CI/HCI-Geräte einsehen.

21. Welche Produkte haben Remotezugriffsfunktionen, die vom sicheren Verbindungsgateway verwaltet werden?

Daten-Storage-, Data-Protection- und CI/HCI-Produkte verfügen über Remotezugriffsfunktionen. Autorisiertes technisches Supportpersonal muss die Zwei-Faktor-Authentifizierung verwenden, um aus der Ferne auf verwaltete Geräte zuzugreifen und Probleme zu beheben. Alle Remotesitzungen werden geprüft und können in der On-Premise-Gateway-Managementkonsole des sicheren Verbindungsgateways im Abschnitt „Audit“ angezeigt werden. Kunden können für zusätzliche Kontrollen und erweiterte Auditfunktionen einen Server für das Policy-Management einrichten, über den sie alle Remotezugriffe flexibel blockieren oder zulassen können.

22. Was ist der Policy Manager für das sichere Verbindungsgateway?

Der Policy Manager für das sichere Verbindungsgateway ist eine separate und kostenfreie externe Software, die für erweiterte Auditfunktionen installiert werden kann. Mit dem Policy Manager können Sie Richtlinien für Remotesupport, Dateiübertragung und/oder Remoteaktionen für Produkte einrichten, die mindestens eine dieser Remotezugriffsfunktionen unterstützen.

Tipp: Eine Vorschau dieser Funktionen finden Sie im Modul *M6 Virtual Edition – Policy-Management* im interaktiven Demo. Sehen Sie sich außerdem technische Anleitungsvideos für die Virtual Appliance Edition an.

23. Wie nutze ich REST APIs?

Mit dem sicheren Verbindungsgateway können Kunden ihr eigenes Scripting mit REST APIs durchführen und unterstützen. Laden Sie das Benutzerhandbuch für REST APIs aus unserem Dokumentationsabschnitt herunter.

Funktionshighlights: OpenManage Enterprise-Umgebung für PowerEdge-Server

24. Welche Systeme werden vom Konnektivitäts-Plug-in für OpenManage Enterprise unterstützt?

PowerEdge-Server und -Gehäuse der 12. bis 15. Generation mit iDRAC und Chassis Management Controller (CMC) sowie Linux-Server werden unterstützt. Erfahren Sie mehr über die unterstützten Produkte und rufen Sie technische Ressourcen ab.

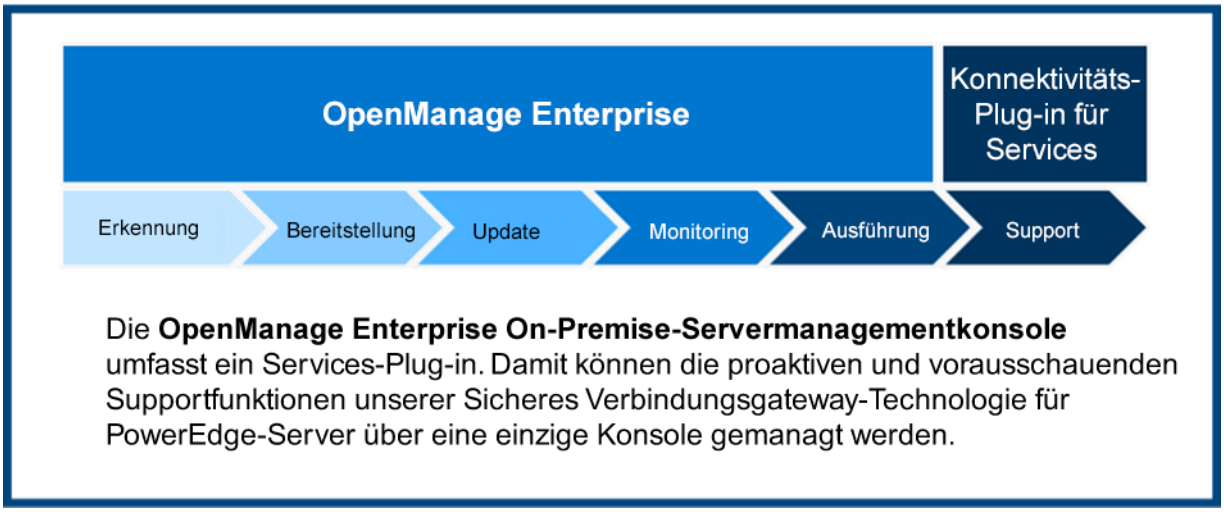
25. Welche Voraussetzungen gelten für das Monitoring der Konnektivität von PowerEdge-Geräten?

Das Plug-in für OpenManage Enterprise und die Gatewayeditionen ermöglichen das Out-of-Band-Monitoring von PowerEdge-Servern ab der 12. Generation (bei Verwendung von iDRAC7, iDRAC8 und iDRAC9) sowie PowerEdge-Gehäusen. Weitere Informationen finden Sie in der Supportmatrix des jeweiligen Geräts.

Alternativ wird das In-Band-Management von PowerEdge-Server unterstützt, wobei vorausgesetzt wird, dass der OpenManage Server Administrator-Agent (OMSA) auf dem Gerät installiert ist und ausgeführt wird. Die empfohlene Version von OMSA variiert je nach Betriebssystem, das auf dem Gerät ausgeführt wird.

26. Inwiefern ergänzt die Konnektivität für Services das Lebenszyklusmonitoring des Rechenzentrumsmanagements von OpenManage Enterprise?

OpenManage Enterprise ist eine benutzerfreundliche 1:n-Systemmanagementkonsole. Damit wird das umfassende Lebenszyklusmanagement für PowerEdge-Server und -Gehäuse in einer Konsole kostengünstig unterstützt. Das Diagramm unten zeigt, wie das Konnektivitäts-Plug-in für OpenManage Enterprise-Services die OpenManage Enterprise-Erfahrung im Rechenzentrum ergänzt. Diese Funktion ist derzeit über das OpenManage Enterprise SupportAssist-Plug-in 1.x und unser aktuelles OpenManage Services-Plug-in 1.x verfügbar. Erfahren Sie mehr und rufen Sie Ressourcen ab.



Sicherheitsinformationen

27. Wo finde ich weitere Informationen zur Sicherheitsarchitektur der Konnektivitätstechnologie?

Laden Sie das Whitepaper zum Thema Sicherheit herunter, um zu erfahren, wie Data Protection und Bedrohungsschutz im sicheren Verbindungsgateway in eine sichere, automatisierte Supporterfahrung integriert sind.

Darin werden folgende Themen behandelt:

- **Sichere Datenerhebung vor Ort:** Erfahren Sie, wie das sichere Verbindungsgateway 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 sichere Verbindungsgateway mithilfe von Verschlüsselung und bilateraler Authentifizierung einen sicheren TLS-Tunnel (Transport Layer Security) für Heartbeat-Abfragen, Remotebenachrichtigungen und Remotezugriffsfunktionen erstellt.

- **Sichere Datenspeicherung und -nutzung und sichere Prozesse:** Hier erfahren Sie mehr über die täglich implementierten Maßnahmen zum Schutz Ihrer Daten, einschließlich physischer Sicherheit, Risikomanagement für Lieferketten und sicherer Entwicklungsprozesse.