

Connettività per i sistemi di infrastrutture Dell

Sommaro

Argomento	Domande frequenti
Introduzione	<ol style="list-style-type: none"> 1. Che cos'è la piattaforma tecnologica Secure Connect Gateway? 2. Esistono altri modi per connettersi, oltre all'opzione gateway? 3. Il software legacy (SupportAssist Enterprise e Secure Remote Services) è stato dismesso? 4. Questo software è installabile e aggiornabile dal cliente? 5. Ho bisogno di una licenza?
Caratteristiche e valore della tecnologia	<ol style="list-style-type: none"> 6. In che modo l'utilizzo del software di connettività offre più valore dall'esperienza di supporto Dell?
Opzioni di deployment della tecnologia	<ol style="list-style-type: none"> 7. In quali modi potete implementare e configurare il software di connettività nel vostro ambiente? 8. Quale software gateway è consigliato per il mio ambiente e quali sono i requisiti minimi? 9. Devo registrare il dispositivo Secure Connect Gateway con Dell Technologies? 10. Quale tecnologia gateway offre funzionalità di supporto remoto? E quali prodotti dispongono di funzionalità di accesso remoto gestite da Secure Connect Gateway? 11. Che cos'è il software Policy Manager e come viene utilizzato per l'opzione gateway? 12. Quali prodotti sono abilitati per la connessione diretta? Posso utilizzare la connessione diretta anche con un gateway? 13. Che cos'è il plug-in Services per OpenManage Enterprise? 14. Come posso ottenere assistenza durante il deployment della connettività software? 15. In caso di problemi, come faccio a contattare il supporto?
Sicurezza	<ol style="list-style-type: none"> 16. Vorrei saperne di più su questo software nell'ambiente del cliente e sulla connessione a Dell. In che modo viene protetto? 17. Come viene gestito il supporto remoto? Chi può accedere al sistema da Dell tramite una sessione di supporto remoto? 18. Per quanto riguarda la sicurezza, queste informazioni di telemetria e eventi dei dati dello stato del sistema vengono sottoposte a verifica? Qual è il ruolo del Policy Manager? 19. Dove posso trovare altre informazioni sull'architettura della sicurezza della tecnologia di connettività?
Scenari di configurazione	<ol style="list-style-type: none"> 20. Quali sono le considerazioni per il deployment e la configurazione della tecnologia di connettività in base alle esigenze dell'azienda?

Sommario - continua

Argomento	Domande frequenti
Servizi di supporto	21. In che modo la connettività è rilevante ai fini del valore del contratto per i servizi di supporto sui prodotti per l'infrastruttura Dell? 22. Che cosa accade alle funzioni di supporto automatizzate quando la copertura contrattuale per i servizi di supporto, ad esempio con ProSupport Infrastructure Suite, scade sul sistema monitorato?
Connettività per PowerEdge	23. Quali sono i modi migliori per implementare e configurare questo software di connettività per server? Come decidete quale strumento utilizzare? 24. In che modo la connettività per i servizi integra il monitoraggio del ciclo di vita della gestione dei data center di OpenManage Enterprise? 25. Quali sistemi sono supportati dal plug-in Services per OpenManage Enterprise?
Altri punti salienti generali	26. Dove è possibile reperire informazioni sulle policy di avviso per Secure Connect Gateway? Quando vengono aperte richieste di assistenza predittive per gli errori hardware? 27. Che cosa è necessario sapere sulle funzionalità di gestione delle credenziali di Secure Connect Gateway? 28. Quali sono le caratteristiche principali della modalità di manutenzione? 29. Secure Connect Gateway consente di impostare le preferenze di notifica e-mail? 30. Quali lingue sono supportate nel dashboard di gestione del gateway on-premise? 31. Cosa devo fare per iniziare a utilizzare le API REST? 32. In che modo viene utilizzato questo software per la connettività per APEX AIOps Infrastructure Observability (in precedenza CloudIQ)?

Introduzione

1: Che cos è la piattaforma tecnologica Secure Connect Gateway?

La nostra [tecnologia Secure Connect Gateway 5.x](#) è l'innovativo software di connettività di Dell Technologies Services.

Offre un'unica soluzione di connettività per la gestione dell'intero portafoglio di infrastrutture Dell, ad esempio server, rete, storage dei dati, protezione dei dati, soluzioni di converged e hyper-converged infrastructure (CI/HCI). Inoltre, sostituisce i software legacy, SupportAssist Enterprise e Secure Remote Services, le cui funzionalità sono integrate in questa tecnologia.

Forniamo **opzioni di deployment flessibili, installabili e aggiornabili dal cliente**. Con un'opzione gateway (fornita come appliance virtuale, applicazione standalone o edizione container), un'opzione di connessione diretta e un'opzione plug-in, puoi scegliere ciò che è adatto per il tuo ambiente.

La nostra tecnologia, **nota anche come software di monitoraggio e supporto IT remoto**, offre:

- Informazioni dettagliate sui problemi più critici
- Risoluzione più rapida dei problemi con accesso remoto e comunicazioni bidirezionali sicure tra Dell Technologies e l'ambiente del cliente
- Un'attenzione continua alla sicurezza con software Policy Manager dotato di funzionalità avanzate di verifica e controllo, il miglior protocollo MQTT del settore e nuovi processi di sviluppo
- Prestazioni e scalabilità migliorate grazie al gateway che gestisce ancora più dati e azioni di telemetria nell'ambiente Dell Enterprise.
- Un'esperienza di interfaccia utente web migliorata per il dashboard di gestione della connettività on-premise

Dopo aver acquistato un prodotto per l'infrastruttura Dell bundled nel contratto per i servizi di supporto, ad esempio con qualsiasi livello di servizio di [ProSupport Infrastructure Suite](#), puoi impostare gratuitamente questo software di connettività. Non è richiesta alcuna licenza.

Una volta che il nostro software monitora questi sistemi, ti forniamo la nostra integrazione esclusiva di AI più intelligente, supporto automatizzato e analisi in tempo reale.

2: Esistono altri modi per connettersi, oltre all'opzione gateway?

Sì. La tecnologia Secure Connect Gateway è stata implementata anche come versione con connessione diretta per determinati componenti hardware Dell e come plug-in.

Alcuni prodotti Dell possono connettersi direttamente al back-end Dell Technologies e sono adatti per i clienti che non desiderano configurare software separato. Consulta la documentazione del prodotto. *Leggi D12 for additional details.*

Per i clienti di un data center PowerEdge che utilizzano OpenManage, ora ci si può connettere al plug-in Services per [OpenManage Enterprise](#) per le funzionalità di avviso, invio automatico e raccolta.

Esplora la tecnologia: visita [Dell.com](#) per conoscere le indicazioni dei nostri esperti e accedere alle risorse tecniche

Infografica con link principali: [Guida introduttiva alla connettività nel data center](#)

3: Il software legacy (SupportAssist Enterprise e Secure Remote Services) è stato dismesso?

Le **edizioni Virtual e Docker di Secure Remote Services v3.x** sono state completamente dismesse il 31 gennaio 2024. Il supporto intelligente e automatizzato per i sistemi di storage, rete e CI/HCI Dell supportati è stato interrotto.

- Nota: per i clienti con **prodotti Dell PowerStore e Unity che utilizzano la connessione diretta**, la tecnologia verrà dismessa il 31 dicembre 2024. Per evitare interruzioni del servizio, un aggiornamento dell'ambiente operativo verrà reso disponibile prima dell'EOSL.

SupportAssist Enterprise 4.x e 2.x sono stati dismessi il 31 luglio 2022. Il supporto intelligente e automatizzato per server, storage, rete e/o sistemi CI/HCI Dell è stato interrotto.

4: Questo software è installabile e aggiornabile dal cliente?

Sì. Puoi scaricare e installare la nostra tecnologia di connettività senza l'assistenza di Dell Technologies.

Visita il sito Dell Support per le risorse software [gateway](#) e [plug-in](#).

- **Suggerimento:** esplora la nostra [demo tecnica interattiva](#) (solo in inglese) per conoscere in anteprima l'installazione, la registrazione e l'utilizzo delle edizioni gateway e del software Policy Manager

5: Ho bisogno di una licenza?

Non è richiesta alcuna licenza software. Tuttavia, per scaricare e registrare il software, è necessario essere autenticati presso il supporto Dell.com.

Caratteristiche e valore della tecnologia

6: In che modo l'utilizzo del software di connettività offre più valore dall'esperienza di supporto Dell?

I motivi principali per cui le aziende utilizzano i nostri strumenti di connettività sono la limitazione dei downtime nel loro ambiente, la riduzione delle attività di monitoraggio dei problemi critici e l'identificazione e la risoluzione di problemi minori prima che diventino più grandi e costosi.

La configurazione della connettività migliora l'esperienza di supporto per i prodotti dell'infrastruttura Dell con la copertura dei servizi di supporto, ad esempio con qualsiasi livello di servizio per [ProSupport Infrastructure Suite](#). Una volta che la nostra tecnologia Secure Connect Gateway, implementata come opzione di gateway, connessione diretta o plug-in, monitora questi sistemi nel tuo ambiente, ti forniamo supporto proattivo, preventivo e, in alcuni casi, predittivo.

I dati sono la linfa vitale della nostra tecnologia di connettività. **Utilizziamo i dati sullo stato del sistema raccolti dagli ambienti dei clienti e provvediamo a correlarli con anni di dati su incidenti e progettazione** provenienti dai team di supporto tecnico e sul campo, nonché dai produttori di componenti. Utilizzando **sofisticati modelli di intelligenza artificiale, tra cui l'apprendimento automatico**, la nostra tecnologia di connettività è in grado di trovare e applicare modelli alla telemetria e ai dati degli eventi per rilevare con precisione il problema su cui agire.

La nostra tecnologia identifica i problemi hardware e software, **crea un caso e avvia un contatto per iniziare a risolvere un problema prima che diventi gravoso**. A seconda del tipo di problema, l'avviso può anche **avviare una spedizione automatica dei componenti**, il che significa una ricezione più rapida dei componenti hardware.

Un'altra straordinaria funzionalità è il **supporto remoto** incluso nella maggior parte dei nostri prodotti di storage, protezione dei dati e converged e hyper-converged infrastructure (CI/HCI). In questo scenario, quando viene aperto un caso da parte nostra, se è possibile risolvere i problemi tramite il supporto remoto, la tecnologia consente una comunicazione bidirezionale sicura per gli agenti autorizzati del supporto tecnico che possono accedere da remoto ai dispositivi gestiti per diagnosticare e risolvere i problemi.

Inoltre, inviando i dati di telemetria a Dell, i **dati cronologici del sistema possono contribuire a ridurre il tempo di risoluzione dei problemi** quando viene coinvolto il supporto Dell. Ad esempio, quando un avviso viene inviato a Dell, un tecnico del supporto può connettersi al dispositivo (in base alle policy impostate dal cliente), quindi confermare le azioni da intraprendere e fornire al cliente un piano d'azione. Ad esempio, è possibile sostituire i componenti prima che si guastino effettivamente, riducendo al minimo il rischio di downtime.

Un altro vantaggio delle funzioni di supporto remoto sono gli **aggiornamenti remoti**. Questo è un ottimo esempio di come utilizziamo la nostra connessione sicura. Molti prodotti possono avere un codice di aggiornamento o patch di sicurezza inviati direttamente al cliente per poterli applicare in base alle proprie esigenze. In alternativa, i nostri team di gestione delle modifiche da remoto possono pianificare ed eseguire l'aggiornamento dall'inizio alla fine senza essere on-site.

Ascolta i suggerimenti dei nostri esperti:

- Ascolta il podcast (solo in inglese): [Ottimizzazione del tempo di attività del data center con il supporto intelligente](#)
- Ascolta il podcast (solo in inglese): [Ottimizzazione dell'uptime di PowerEdge con il supporto proattivo e predittivo](#)

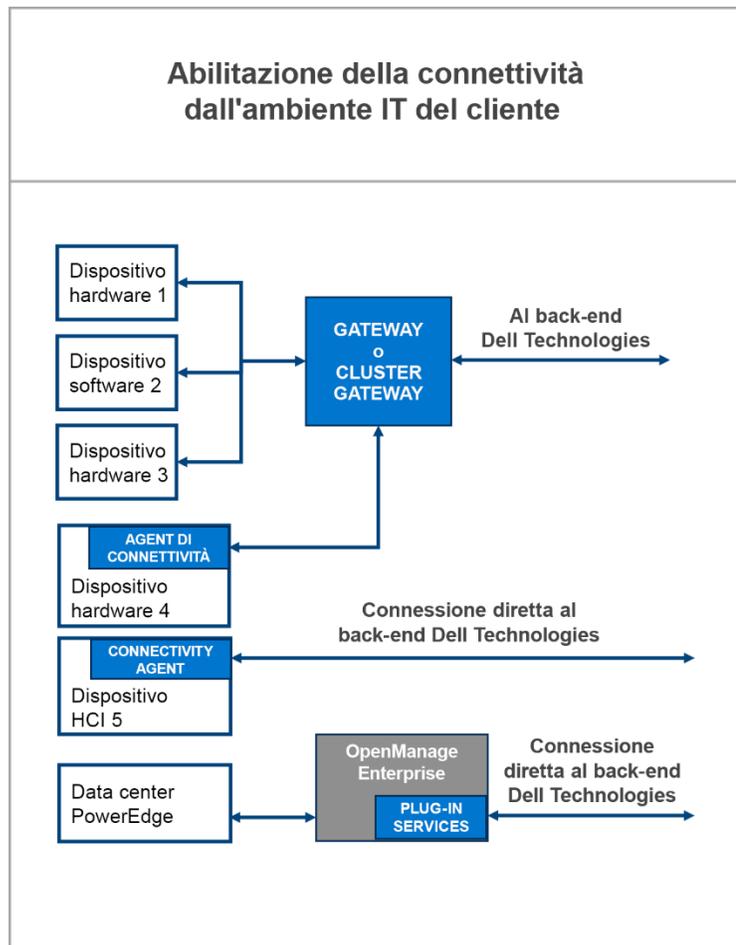
Guarda i brevi video (solo in inglese):

- [Caratteristiche e vantaggi della connettività](#)
- [Architettura e funzionalità di protezione](#)

Opzioni di deployment della tecnologia

7: In quali modi potete implementare e configurare il software di connettività nel vostro ambiente?

Puoi scegliere ciò che è più adatto al tuo ambiente con le nostre opzioni di installazione flessibili: un'opzione gateway, un'opzione di connessione diretta e un'opzione plug-in. Tutti sono installabili e aggiornabili dal cliente.



L'opzione **Secure Connect Gateway** consente di connettere i sistemi Dell al gateway per comunicare con Dell Technologies Services. In questo modo si semplifica la configurazione del firewall/rete in modo che il gateway sia l'unica cosa che si connette in uscita su Internet.

Per la nostra opzione gateway, Dell fornisce **un'edizione virtuale** per ambienti VMware e Hyper-V. Sono inoltre disponibili **versioni container** per ambienti Docker, Podman e Kubernetes. Per i nostri clienti server più piccoli, forniamo **un'edizione per applicazioni** con versioni Windows/Linux. *Vedi D8-11.*

I clienti che desiderano high availability e failover per i propri sistemi possono configurare più gateway o un cluster che fornirà ridondanza nel caso in cui un gateway non sia disponibile.

L'**opzione di connessione diretta** (abilitata integrando la nostra tecnologia di connettività nell'ambiente operativo del prodotto Dell) è destinata ai clienti di piccole dimensioni e non tradizionali che potrebbero non voler configurare software aggiuntivo. *Maggiori informazioni nel Q12.*

Infine, per i nostri clienti incentrati sull'elaborazione, abbiamo il **plug-in Services per OpenManage Enterprise** per la flotta di server PowerEdge per un'unica connessione diretta sicura. *Maggiori informazioni nel Q13 e nel Q23-25.*

Infografica con link principali: [Guida introduttiva alla connettività nel data center](#)

7 (continua): In quali modi potete implementare e configurare il software di connettività nel vostro ambiente?

Fai riferimento alla tabella per selezionare l'opzione appropriata per l'ambiente in uso. Verifica la Support Matrix del prodotto per [Secure Connect Gateway](#) oppure visita la pagina di supporto dei prodotti hardware all'indirizzo Dell.com/Support. La versione dell'applicazione è ideale per i clienti con sistemi di dimensioni minori che non dispongono di un ambiente virtualizzato e utilizzano l'hardware e il software supportati elencati di seguito.

Connessione per il monitoraggio di tutti i dispositivi da un'unica posizione

Soluzioni integrate	Hardware e software supportati
Secure Connect Gateway 5.x – Edizione per appliance virtuali <i>Per VMware e Microsoft HyperV</i> <i>Pacchetti container: Docker, Podman, Kubernetes</i>	Intero portafoglio di prodotti Dell: storage dei dati, server, rete, CI/HCI e protezione dei dati
Secure Connect Gateway 5.x – Edizione per applicazioni <i>Gestione di Windows Enterprise su server</i> <i>Gestione di Linux su server</i>	PowerEdge, iDRAC, PowerSwitch, Webscale, PeerStorage, EqualLogic, Compellent, FluidFS (Fluid File System) e PowerVault
Plug-in Services di OpenManage Enterprise <i>Per l'ambiente OpenManage Enterprise</i>	Server PowerEdge

Connessione diretta per prodotti hardware Dell specifici

- Integrazione della connettività nell'ambiente operativo del prodotto Dell. Verificare il prodotto Dell Documentazione di supporto per verificare il modello e la versione specifici del prodotto.
- Soluzione appropriata per il deployment eterogeneo di più prodotti hardware Dell.
- Connessione diretta a Dell Technologies o tramite il server Secure Connect Gateway

Infografica con link principali: [Guida introduttiva alla connettività nel data center](#)

8: Quale software gateway è consigliato per il mio ambiente e quali sono i requisiti minimi?

Software gateway	
<p>Secure Connect Gateway - Edizione virtuale</p> <p>Sono disponibili versioni per:</p> <ul style="list-style-type: none"> Ambiente VMware/Ambiente Microsoft HyperV Pacchetti container: Docker, Podman, Kubernetes <p>Scarica la documentazione e tutte le risorse dal sito Dell.com/Support.</p>	<p>Secure Connect Gateway - Edizione per applicazioni</p> <p>Sono disponibili versioni per:</p> <ul style="list-style-type: none"> Server di gestione Windows (monitoraggio di dispositivi Windows e Linux) Server di gestione Linux (monitoraggio di dispositivi Linux) <p>Scarica la documentazione e tutte le risorse dal sito Dell.com/Support.</p>
<p>Visualizza in anteprima la demo tecnica interattiva per suggerimenti tecnici sull'installazione, la registrazione e l'utilizzo.</p>	
<p>Assicurati di esaminare i requisiti minimi per l'installazione e l'utilizzo del software Secure Connect Gateway</p>	

Quattro passaggi per connettere i clienti

1

Preparazione del sito e verifica dell'account

Anteprima dei requisiti tecnici e pianificazione con l'amministratore di rete. Prima del passaggio 2, configura un [account aziendale](#) su Dell.com/Support.

2

Download

Accedi con le credenziali dell'account alla [pagina di supporto del prodotto](#) per Secure Connect Gateway su Dell.com/Support. Scarica l'edizione corretta per l'ambiente del cliente e crea la chiave di accesso per l'autenticazione

3

Installazione e provisioning

Implementa il modello dell'appliance virtuale o installa il software applicativo. Completa i passaggi per la registrazione iniziale.

4

Connessione dei dispositivi

Configura e abilita le comunicazioni tra i prodotti Dell e il server gateway

Suggerimenti per i nuovi utenti al primo utilizzo:

- I nuovi clienti devono innanzitutto [impostare un account aziendale enterprise](#) all'indirizzo Dell.com/Support. Nella pagina di download di Secure Connect Gateway ti verrà richiesto di effettuare l'accesso e completare questo passaggio.
- Al termine dell'operazione, accedi con le credenziali del tuo account alla [pagina del supporto del prodotto Secure Connect Gateway](#) su Dell.com/Support.
- Assicurati di inserire la posizione del sito per l'installazione del software. Questo ci aiuta a fornire un'esperienza di supporto migliore.
- Scarica l'edizione corretta per il tuo ambiente. Durante questo passaggio dovrai creare la chiave di accesso per l'autenticazione.

Nota: per coloro che si collegano per la prima volta in assoluto, la preparazione del sito richiederà più tempo. Da giorni a potenzialmente mesi, a seconda della complessità delle policy di rete e di sicurezza. I team di sicurezza e di rete potrebbero richiedere una revisione del prodotto prima dell'implementazione. Leggi il nostro [white paper sulla sicurezza](#).

Esplora la tecnologia: visita Dell.com per conoscere le indicazioni dei nostri esperti e accedere alle risorse tecniche.

Bisogno di aiuto? Puoi rivolgerti agli esperti nel [forum di Secure Connect Gateway](#)

9: Devo registrare il dispositivo Secure Connect Gateway con Dell Technologies?

Sì. Per utilizzare Secure Connect Gateway e ricevere la migliore sicurezza della categoria, devi effettuare la registrazione con Dell Technologies.

Suggerimento: scopri come [configurare un account aziendale](#). Se viene visualizzato un segno di spunta nero accanto al nome in Dell.com/Support, l'autenticazione è andata a buon fine.

Utilizza l'account aziendale per accedere alla pagina di download, generare una chiave di accesso e un pin, quindi usa la chiave di accesso e il pin per attivare il Secure Connect Gateway.

Ai clienti che non dispongono di un account business verranno chieste ulteriori informazioni sulla propria organizzazione e sui propri prodotti. Il cliente potrà continuare dopo aver eseguito il processo di verifica.

10: Quale tecnologia gateway offre funzionalità di supporto remoto? E quali prodotti dispongono di funzionalità di accesso remoto gestite da Secure Connect Gateway?

Le funzionalità di supporto remoto sono disponibili solo nelle edizioni virtuale e container di Secure Connect Gateway e *non sono disponibili nell'edizione per applicazioni*.

I prodotti per lo storage e la protezione dei dati e converged e hyper-converged infrastructure (CI/HCI) dispongono di funzionalità di accesso remoto. I prodotti PowerEdge e PowerSwitch possono anche essere abilitati per il supporto remoto nell'interfaccia utente di gestione del gateway on-premise tramite la panoramica del dispositivo.

Gli agenti autorizzati del supporto tecnico utilizzano l'autenticazione a due fattori obbligatoria per accedere da remoto ai dispositivi gestiti e risolvere i problemi. Tutte le sessioni remote vengono sottoposte ad audit ed è possibile accedere ai dettagli dalla console di gestione del gateway on-premise per Secure Connect Gateway, nella sezione Audit.

Per un maggiore controllo e funzionalità di verifica avanzate, i clienti possono configurare un server di gestione delle policy che offre la flessibilità di bloccare o consentire tutte le sessioni di accesso remoto.

11: Che cos'è il software Policy Manager e come viene utilizzato per l'opzione gateway?

Policy Manager per Secure Connect Gateway è un software esterno separato e gratuito che può essere installato per sfruttare funzionalità avanzate di verifica e controllo remoto.

Policy Manager permette di impostare le policy per il supporto remoto, il trasferimento di file e/o le azioni remote per i prodotti che supportano una o più di queste funzionalità di accesso remoto.

Nota: Policy Manager può essere utilizzato solo con le edizioni virtuale e container del gateway. Non è disponibile per l'edizione per applicazioni.

Suggerimenti: visualizza in anteprima il modulo di gestione delle policy nella [demo interattiva](#). Guarda i video tecnici per l'edizione per [appliance virtuali](#).

12: Quali prodotti sono abilitati per la connessione diretta? Posso utilizzare la connessione diretta anche con un gateway?

In alcuni casi, la nostra tecnologia di connettività è integrata nell'ambiente operativo del prodotto Dell e consente la connessione diretta al back-end dei nostri servizi. Questo è ciò che si intende per "connessione diretta".

Ti verrà richiesto di abilitare i servizi di connettività durante la configurazione dei prodotti hardware e software Dell.

Tuttavia, in qualsiasi momento, potrai commutare il prodotto Dell abilitato per la connessione diretta impostando la connessione tramite un gateway. Le policy di sicurezza e di rete dell'azienda influenzeranno le decisioni relative alla configurazione.

Prodotti dell'infrastruttura Dell abilitati per la connessione diretta

Verifica sempre l'elenco più aggiornato dei prodotti supportati su Dell.com/Support

Appsync | APEX AIOps Infrastructure Observability Collector | CMS - software VxBlock
Backup dei dati Avamar | Data Domain | Data Domain Management Console | Edge Orchestrator
Elastic Cloud Storage | Appliance con nodi metro | ObjectScale
Famiglia PowerFlex Family - appliance, rack, software
PowerProtect - Data Manager, appliance Data Manager, appliance scale-out
PowerScale | PowerStore | PowerVault | Serie S5000 | SRM | Streaming dei dati | Unity | VxRail

[Consulta la documentazione di supporto del prodotto per verificare il modello e la versione specifici del prodotto con funzionalità di connessione diretta.](#)

Nota: le funzionalità software di SupportAssist, SupportAssist Enterprise e Secure Remote Services fanno ora parte della nostra piattaforma software di connettività di nuova generazione. Questi riferimenti software nell'interfaccia utente del prodotto verranno aggiornati di conseguenza nel corso del tempo.

13: Che cos'è il plug-in Services per OpenManage Enterprise?

La tecnologia Secure Connect Gateway ora è stata anche implementata come plug-in. Per i clienti di un data center PowerEdge che utilizzano OpenManage, ora ci si può connettere al plug-in Services per [OpenManage Enterprise](#) per le funzionalità di avviso, invio automatico e raccolta.

Risorse:

- [Scopri di più sul plug-in e ottieni le risorse tecniche](#)
- Per conoscere i prodotti supportati, visualizza il documento Support Matrix del prodotto nella [pagina di supporto dei prodotti OpenManage Enterprise Services](#).

Ascolta i suggerimenti dei nostri esperti:

- **Guarda il breve video** (solo in inglese): [Plug-in Services per OpenManage Enterprise](#)

- **Ascolta il podcast** (solo in inglese): [Ottimizzazione dell'uptime di PowerEdge con il supporto proattivo e predittivo](#)
- **Leggi:** [white paper sulla sicurezza](#)

14: Come posso ottenere assistenza durante il deployment della connettività software?

Molti clienti scaricano e installano la nostra tecnologia di connettività senza l'assistenza di Dell Technologies. [Visita la nostra pagina web per tutte le risorse.](#)

Suggerimento: puoi avviare ed esplorare la nostra [demo tecnica interattiva](#)

- *Visualizza in anteprima l'installazione, la registrazione e l'uso delle edizioni gateway e di Policy Manager*

Per i clienti che desiderano assistenza, la suite di servizi [ProDeploy Infrastructure Suite](#) include l'abilitazione e la configurazione di Secure Connect Gateway.

Ai clienti che dispongono di una copertura [ProSupport Plus](#) viene assegnato un Service Account Manager (SAM) che fornirà assistenza con l'installazione e risponderà alle domande relative alla registrazione.

In caso contrario, se necessario, contatta il supporto Dell Technologies per ricevere assistenza.

15: In caso di problemi, come faccio a contattare il supporto?

In caso di problemi con il supporto online di Dell.com o con Secure Connect Gateway, visita la pagina del [Supporto amministrativo da questa posizione](#) per richiedere assistenza. Seleziona la categoria in cui rientra il problema e compila i dettagli come richiesto. Se hai bisogno di assistenza immediata con un [problema di competenza del supporto tecnico](#), contattaci [qui](#). Contatta il tuo Service Account Manager (se applicabile).

Sicurezza

16: Vorrei saperne di più su questo software nell'ambiente del cliente e sulla connessione a Dell. In che modo viene protetto?

La connessione tra l'ambiente e Dell è protetta attraverso un tunnel TLS reciproco e una catena di certificati. In questo tipo di configurazione, i sistemi si connessero al software del tuo ambiente e tali connessioni dovranno essere solo modifiche di porte/reti interne. Il software è l'unica cosa che si connette in uscita tramite Internet e di nuovo a Dell. Funge da punto di aggregazione per tutti i sistemi connessi per gli eventi e i dati di telemetria. Questa è l'unica informazione sullo stato del sistema che viene inviata.

Tutta la telemetria dei sistemi viene trasportata utilizzando HTTPS TLS 1.3. Forniamo inoltre funzionalità di supporto remoto tramite il tunnel sicuro per accedere e risolvere i problemi del sistema, velocizzando la risoluzione dei problemi ed evitando il downtime.

Scopri di più nel nostro [white paper sulla sicurezza](#).

17: Come viene gestito il supporto remoto? Chi può accedere al sistema da Dell tramite una sessione di supporto remoto?

Da Dell, i nostri ingegneri del supporto tecnico utilizzano un portale per creare sessioni di supporto remoto per accedere ai sistemi dei clienti per la risoluzione dei problemi e per le attività di upgrade. Utilizzano l'autenticazione a più fattori per accedere a questo portale. Questi membri del team Dell devono seguire una formazione rigorosa e richiedere l'approvazione della direzione per l'accesso. Utilizziamo il protocollo MQTT, una soluzione ampiamente accettata per i sistemi aziendali connessi, come agente di supporto remoto.

18: Per quanto riguarda la sicurezza, queste informazioni di telemetria e eventi dei dati dello stato del sistema vengono sottoposte a verifica? Qual è il ruolo del Policy Manager?

Controlliamo tutte le transazioni e, nel software, puoi visualizzare queste informazioni nell'interfaccia utente. Tutte le sessioni di supporto remoto e gli eventi e i trasferimenti di telemetria sono disponibili per la visualizzazione.

Per i clienti con policy di sicurezza più rigorose o con revisori di terze parti che richiedono l'archiviazione di queste informazioni per un periodo di tempo prolungato, consigliamo di configurare il nostro software Policy Manager. Policy Manager opera con Secure Connect Gateway per fornire funzioni avanzate di verifica e controllo del supporto remoto. *Vedi anche D11.*

19: Dove posso trovare altre informazioni sull'architettura della sicurezza della tecnologia di connettività?

Scarica il [white paper sulla sicurezza](#) per scoprire come Secure Connect Gateway integra la protezione dei dati e la prevenzione delle minacce in un'esperienza di supporto automatizzata e sicura.

Il documento illustra:

- **Data collection on-site sicura:** informazioni su come Secure Connect Gateway funge da broker per la sicurezza delle comunicazioni, consente ai clienti di controllare i requisiti di autorizzazione, utilizza i protocolli di autenticazione a due fattori e offre altre utili funzionalità.
- **Trasporto e comunicazione sicuri dei dati:** informazioni su come Secure Connect Gateway utilizza la crittografia e l'autenticazione bilaterale per creare un tunnel TLS sicuro per le funzioni di polling di heartbeat, notifica remota e accesso remoto.
- **Storage, utilizzo e processi sicuri dei dati:** ulteriori informazioni sulle serie di misure implementate quotidianamente per proteggere i dati tra cui sicurezza fisica, gestione dei rischi della supply chain e processi di sviluppo sicuri.

Ascolta i suggerimenti dei nostri esperti:

- **Ascolta il podcast** (solo in inglese): [Ottimizzazione dell'uptime del data center con il supporto intelligente](#)
- **Leggi:** [white paper sulla sicurezza](#)

Guarda i brevi video (solo in inglese):

- [Architettura e funzionalità di protezione](#)
- [Configurazione della sicurezza per ambienti di grandi e piccole dimensioni](#)
- [Funzionalità di protezione per il settore finanziario](#)

In alternativa, guarda il webinar (solo in inglese): Ascolta i suggerimenti [dei nostri esperti in questo evento Spiceworks Community](#) in cui vengono trattati i seguenti argomenti:

- In che modo Secure Connect Gateway integra privacy, protezione dei dati e prevenzione delle minacce
- Come implementare in modo flessibile la connettività in ambienti di piccole e grandi dimensioni e non tradizionali
- Perché il supporto automatizzato aiuta a prevenire e mitigare i problemi per i sistemi connessi

Scenari di configurazione

20: Quali sono le considerazioni per il deployment e la configurazione della tecnologia di connettività in base alle esigenze dell'azienda?

I primi elementi da prendere in considerazione sono i **tipi di prodotti (elaborazione, storage, protezione dei dati, converged e hyper-converged infrastructure (CI/HCI))** che verranno configurati per la connettività e **l'ambiente corrente**, ad esempio

- I data center sono collegati in rete o no?
- Gestisci l'elaborazione o lo storage (inclusi i prodotti per la protezione dei dati, CI/HCI) *separatamente o insieme?*

Ti consigliamo anche di considerare le **policy di sicurezza e di rete** dell'azienda. Inoltre, **se i tuoi team vogliono gestire tutti i prodotti insieme o preferiscono segmentarli in base alla geolocalizzazione o al tipo di prodotto.**

In sostanza, devi pensare a come le cose sono collegate tra loro, a come i team lavorano insieme e a come ridurre al minimo la complessità della rete. Così facendo sarai in grado di progettare l'architettura più efficace in base alle varie opzioni di deployment.

Leggi e condividi la nostra panoramica sulle [considerazioni per la configurazione della connettività](#) che tratta:

1. Qual è la configurazione consigliata per un'azienda più grande attenta alla sicurezza?
2. Quali sono le opzioni di configurazione e deployment per le organizzazioni di medie e piccole dimensioni?
3. Cosa succede se sono un'azienda di grandi e medie dimensioni con un'ambiente incentrato sull'elaborazione? Come faccio a decidere quale strumento utilizzare?
4. Cosa succede se dispongo di ~ 1-50 server PowerEdge senza avere un ambiente virtualizzato? Quali sono le opzioni per il gateway?
5. Cosa succede se ho prodotti Dell con disponibilità di connessione diretta? Quali sono alcuni casi d'uso tipici?
6. Qual è la configurazione più adatta alla mia azienda?

Servizi di supporto

21: In che modo la connettività è rilevante ai fini del valore del contratto per i servizi di supporto sui prodotti per l'infrastruttura Dell?

In breve, ottieni più valore dai contratti di supporto attivi sui sistemi Dell implementando il nostro software di connettività nel tuo ambiente e collegando i dispositivi Dell che saranno monitorati da questo software. È un software libero, non è necessaria alcuna licenza. Supportiamo oltre 90+ prodotti dell'infrastruttura Dell: hardware e software. Potrai trarre vantaggio dalla nostra esclusiva integrazione di AI più intelligente, supporto automatizzato e analisi in tempo reale.

I clienti che sfruttano i servizi [ProSupport Infrastructure Suite](#) ricevono un valore importante a tutti i livelli.

- Ulteriori informazioni: [Copertura ProSupport e ProSupport Plus per sistemi di infrastruttura Dell](#)
 - Learn more: [Lifecycle Extension with ProSupport o ProSupport Plus](#)
- Nota: [i sistemi Dell con Basic Hardware Support \(giorno lavorativo successivo alla chiamata\)](#) possono usufruire delle nostre funzionalità di rilevamento proattivo e personalizzato dei problemi, di creazione dei casi e di notifica se monitorati dal nostro software di connettività. Quando viene rilevato un problema, i clienti Basic Support ricevono un'e-mail con il numero del caso e viene loro richiesto di contattare in modo tempestivo il supporto Dell per confermare di voler ricorrere all'assistenza Dell per la risoluzione del problema.

Esplora anche i nostri [servizi di supporto specializzati per l'infrastruttura](#)

22: Che cosa accade alle funzioni di supporto automatizzate quando la copertura contrattuale per i servizi di supporto, ad esempio con ProSupport Infrastructure Suite, scade sul sistema monitorato?

Se il contratto di assistenza per un qualsiasi livello di ProSupport Infrastructure Suite scade, la funzionalità di creazione automatica di richieste verrà disabilitata. La tecnologia Secure Connect Gateway implementata come gateway, come connessione diretta o come plug-in continuerà tuttavia a eseguire raccolte automatizzate delle informazioni sullo stato del sistema. Se esegui l'upgrade o estendi il contratto su un sistema (codice di matricola), la creazione automatica delle richieste verrà automaticamente riabilitata automaticamente sul sistema specifico.

Connettività per PowerEdge

23: Quali sono i modi migliori per implementare e configurare questo software di connettività per server? Come decidete quale strumento utilizzare?

In sintesi, il plug-in Services nella soluzione [OpenManage Enterprise](#) è ideale per i clienti con ambienti incentrati sull'elaborazione, mentre la soluzione gateway rappresenta la strada da percorrere per la gestione di una varietà di prodotti per l'infrastruttura Dell.

Entrambe le soluzioni includono le funzionalità di avviso, creazione automatica di casi, invio automatico e raccolta di telemetria per i server PowerEdge che dispongono di un contratto di supporto.

La scelta dipende dal tipo di ambienti in uso, dal collegamento di rete tra questi ambienti, dai tipi di dispositivi monitorati e dalle preferenze dell'utente.

Se hai configurato o stai pensando di configurare OpenManage Enterprise, il [plug-in Services](#) è la soluzione giusta per te. OpenManage Enterprise è la soluzione di infrastruttura Dell che facilita la gestione del ciclo di vita di migliaia di server PowerEdge da un'unica console.

- Per chi non ha familiarità con questa soluzione, è sufficiente installare Open Manage Enterprise nel proprio ambiente, integrare i prodotti server e quindi installare il plug-in Services, assicurandosi che il firewall sia configurato correttamente, in modo che inizi a inviare avvisi e telemetria a Dell.

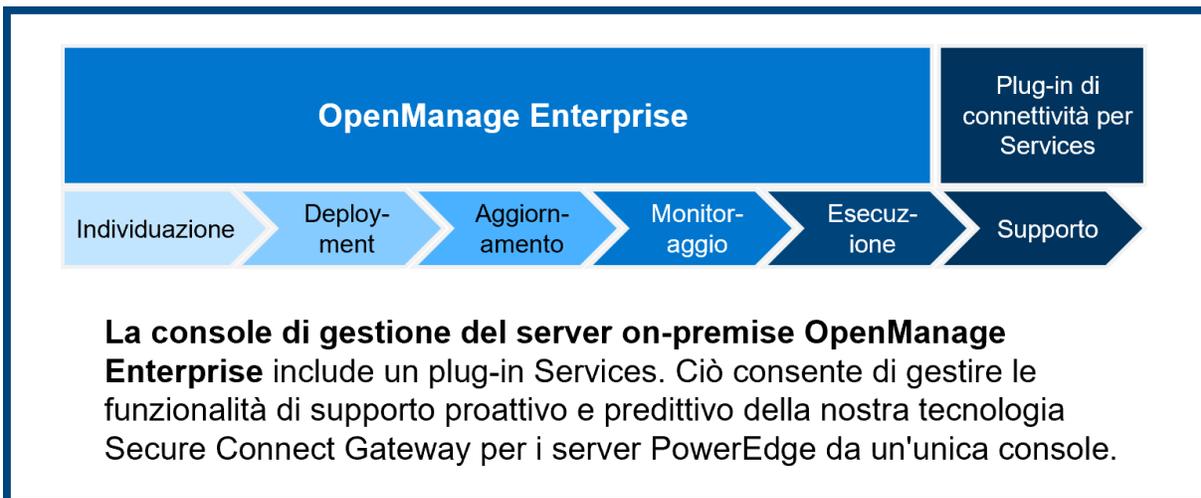
Per i clienti con una combinazione di prodotti per l'infrastruttura Dell, come Powerstore, PowerMax, PowerScale, Data Domain e VxRail, in esecuzione insieme a PowerEdge, consigliamo di configurare la soluzione [Secure Connect Gateway](#) per gestire tali sistemi da un'unica interfaccia utente.

Ascolta i suggerimenti dei nostri esperti:

- **Ascolta il podcast** (solo in inglese): [Ottimizzazione dell'uptime di PowerEdge con il supporto proattivo e predittivo](#)
 - Cosa comporta la connessione dei sistemi PowerEdge tramite la soluzione OpenManage Enterprise e confronto con la connessione tramite una soluzione gateway
 - Come collegarsi ai dispositivi PowerEdge stessi
 - Come scalare facilmente il numero di server connessi nel tempo
 - Altri scenari di configurazione: esecuzione di entrambe le opzioni plug-in e gateway

24: In che modo la connettività per i servizi integra il monitoraggio del ciclo di vita della gestione dei data center di OpenManage Enterprise?

[OpenManage Enterprise](#) è una console di gestione dei sistemi uno-a-molti semplice da usare. Semplifica in maniera efficiente in termini di costi la gestione completa del ciclo di vita di server e chassis PowerEdge in un'unica console. Esamina il diagramma di seguito per comprendere in che modo il plug-in di connettività per OpenManage Enterprise integra l'esperienza OpenManage Enterprise per il data center. Ciò è attualmente disponibile tramite il plug-in Services per OpenManage Enterprise. [Scopri di più e trova le risorse.](#)



25: Quali sistemi sono supportati dal plug-in Services per OpenManage Enterprise?

Sono supportati server e chassis PowerEdge con iDRAC e Chassis Management Controller (CMC), nonché server Linux.

Per verificare specifici prodotti supportati, visita il sito Dell.com/Support e visualizza il documento Support Matrix nella [pagina del supporto dei prodotti OpenManage Enterprise Services](#).

Altri punti salienti generali

26: Dove è possibile reperire informazioni sulle policy di avviso per Secure Connect Gateway? Quando vengono aperte richieste di assistenza predittive per gli errori hardware?

La [policy sugli avvisi di Secure Connect Gateway](#) fornisce informazioni sugli avvisi che aprono richieste con il supporto tecnico di Dell Technologies. I clienti che utilizzano Secure Connect Gateway riceveranno solo la creazione automatica predittiva di richieste per l'hardware del server (disco rigido, backplane e espansioni) su sistemi con servizi ProSupport Plus. Gli avvisi predittivi si basano su raccolte pianificate che vengono inviate a Dell Technologies.

27: Che cosa è necessario sapere sulle funzionalità di gestione delle credenziali di Secure Connect Gateway?

Secure Connect Gateway offre la flessibilità necessaria per aggiungere più account di credenziali e profili. Gli account di credenziali consentono agli amministratori di aggiungere l'autenticazione per tipo di prodotto. Inoltre, i profili consentono a più amministratori che differiscono per funzione o regione di gestire i propri account specifici. I prodotti in cui le credenziali sono necessarie includono server PowerEdge, iDRAC, Compellent, reti, serie PS, serie MD e sistemi Webscale.

Offriamo anche l'integrazione del vault delle credenziali. Si tratta di un'utilissima funzionalità per i clienti con molti dispositivi, in quanto possono aggiungere sistemi e mantenere le credenziali corrette senza compromettere la sicurezza o aumentare il lavoro manuale. Le API CyberArk Conjur e i prodotti CyberArk Credential Provider sono attualmente supportati. Verranno aggiunti altri fornitori. Consulta la documentazione di supporto per l'elenco più aggiornato.

Suggerimento: visualizza in anteprima queste funzionalità nel modulo *Gestione dei dispositivi* nella [demo interattiva](#).

28: Quali sono le caratteristiche principali della modalità di manutenzione?

Si verifica una "tempesta di eventi" quando si attivano avvisi hardware in rapida successione, superando un limite di conteggio predefinito. In questo scenario, Secure Connect Gateway interromperà l'elaborazione degli avvisi per i dispositivi specifici che hanno attivato la tempesta di eventi. Tutti gli altri dispositivi continueranno a essere monitorati da Secure Connect Gateway per rilevare gli avvisi convalidati che potrebbero creare richieste di assistenza.

Inoltre, gli utenti ora dispongono di un'opzione per abilitare manualmente la manutenzione su uno o più dispositivi dall'interno del sistema. Questa operazione può essere utilizzata per la manutenzione pianificata e implementata quando non si desidera che Secure Connect Gateway monitori tali dispositivi. Una volta completate le attività di manutenzione pianificate, è possibile disabilitare manualmente la modalità di manutenzione per segnalare a Secure Connect Gateway di riprendere il monitoraggio.

29: Secure Connect Gateway consente di impostare le preferenze di notifica e-mail?

Sì. Le preferenze di notifica e-mail possono essere personalizzate tramite l'interfaccia utente di Secure Connect Gateway nella scheda Impostazioni. Consulta [la guida utente per ulteriori informazioni](#).

30: Quali lingue sono supportate nel dashboard di gestione del gateway on-premise?

L'interfaccia del software Secure Connect Gateway è disponibile in inglese, tedesco, portoghese brasiliano, francese, spagnolo, cinese semplificato e giapponese. Tuttavia, i clienti possono scegliere tra 28 lingue per le notifiche email automatiche inviate al momento di un incidente con Service Request. Nota: alcune notifiche e-mail non verranno tradotte nelle lingue locali a causa di limitazioni del sistema operativo.

31: Cosa devo fare per iniziare a utilizzare le API REST?

Con Secure Connect Gateway, i clienti possono eseguire e supportare il proprio scripting personalizzato con API REST. Scarica la guida utente alle API REST dalla [sezione dedicata alla documentazione](#).

32: In che modo viene utilizzato questo software per la connettività per APEX AIOps Infrastructure Observability (in precedenza CloudIQ)?

[APEX AIOps Infrastructure Observability](#) APEX AIOps Infrastructure Observability:(in precedenza CloudIQ) aiuta a ottimizzare l'integrità dell'infrastruttura core, edge e multicloud Dell fornendo informazioni e suggerimenti su integrità, sicurezza informatica e sostenibilità basati sull'AI.

- Gli attributi chiave includono stato di integrità e assessment dei rischi per la sicurezza informatica e raccomandazioni per la correzione; monitoraggio delle prestazioni e della capacità, rilevamento delle anomalie e previsioni; previsione dei guasti; monitoraggio e previsione dell'energia e delle emissioni; e monitoraggio delle risorse di virtualizzazione.

Il nostro software di connettività viene utilizzato esclusivamente per la trasmissione dei dati di sistema ed eventi dall'ambiente del cliente. I dati di telemetria vengono trasmessi in modo sicuro al back-end Dell, dove vengono analizzati dagli algoritmi di intelligenza artificiale per APEX AIOps Infrastructure Observability.

Caratteristiche principali (non correlate alla connettività):

- All'interno del portale di Infrastructure Observability è inoltre possibile sfruttare AIOps Assistant che utilizza l'AI generativa per fornire risposte immediate e dettagliate e suggerimenti per la risoluzione dei problemi per l'infrastruttura Dell.