Dell 인프라스트럭처 시스템 연결

목차

목차 계속

소개

1: 보안 연결 게이트웨이 기술 플랫폼이란 무엇입니까?

Dell secure connect gateway 5.x 기술은 Dell Technologies Services의 차세대 연결 소프트웨어입니다.

서버, 네트워킹, 데이터 스토리지, 데이터 보호, 컨버지드 및 하이퍼 컨버지드(CI/HCI) 솔루션 등 **전체 Dell 인프라스트럭처 포트폴리오를 관리할 수 있는 단일 연결 솔루션**을 제공합니다. 또한 이 기술에 기능이 통합된 기존 소프트웨어인 SupportAssist Enterprise 및 Secure Remote Services를 대체합니다.

고객이 직접 설치하고 업그레이드할 수 있는 유연한 배포 옵션을 제공합니다. 게이트웨이 옵션(가상 어플라이언스, 독립 실행형 애플리케이션 또는 컨테이너 에디션으로 제공), 직접 연결 옵션, 플러그인 옵션을 통해 현재 운영 환경에 적합한 옵션을 선택할 수 있습니다.

원격 IT 지원 및 모니터링 소프트웨어라고도 하는 기술은 다음과 같은 이점을 제공합니다.

- 가장 중요한 문제에 대한 통찰력
- Dell Technologies와 고객 환경 간의 원격 액세스 및 양방향 보안 통신으로 빠른 문제 해결
- 최고 수준의 MQTT 프로토콜과 새로운 개발 프로세스를 갖춘 고급 감사 및 제어 기능이 탑재된 정책 관리자 소프트웨어로 지속적으로 보안을 지원
- Dell 엔터프라이즈 환경 전반에서 더 많은 텔레메트리 데이터 및 작업을 처리하는 게이트웨이를 통해 성능 및 확장성 개선
- Dell EMC에서 제공하는 온프레미스 접속 구성 관리 대시보드의 웹 UI 환경 향상

지원 서비스 계약(예: ProSupport Infrastructure Suite의 모든 서비스 수준)이 번들로 제공되는 Dell 인프라스트럭처 제품을 구매하면 이 연결 소프트웨어를 무료로 설치할 수 있습니다. 라이선스는 필요하지 않습니다.

소프트웨어가 이러한 시스템을 모니터링하기 시작하면 Dell에서 더 스마트한 AI, 자동화된 지원, 실시간 분석이 통합된 고유한 환경을 제공할 수 있게 됩니다.

2: 게이트웨이 옵션을 사용하는 것 외에 연결할 수 있는 다른 방법이 있습니까?

예. Secure Connect Gateway 기술은 일부 Dell 하드웨어 및 플러그인에 대한 직접 연결 버전으로도 구현되었습니다.

일부 Dell 제품은 Dell Technologies 백엔드에 다시 직접 연결할 수 있으며, 별도의 소프트웨어 설치를 원치 않는 고객에게 적합합니다. 관련 내용은 제품 설명서를 참조하시기 바랍니다. *자세한 내용은 Q12 및 Q29을 참조하십시오.*

PowerEdge 데이터 센터에서 OpenManage를 활용하는 고객의 경우, 이제 OpenManage Enterprise 용 플러그인으로 연결하여 알림, 자동 디스패치 및 수집 기능을 사용할 수 있습니다.

기술 살펴보기: Dell.com을 방문하여 전문가의 견해 및 기술 리소스 참조

주요 링크가 포함된 인포그래픽:데이터 센터에서 연결 시작하기

3: 기존 소프트웨어인 SupportAssist Enterprise 및 Secure Remote Services는 사용 중지되었습니까?

Secure Remote Services v3.x의 Virtual Edition과 Docker Edition은 2024년 1월 31일에 서비스가 완전히 중단되었습니다. 지원되는 Dell 스토리지, 네트워킹 및 CI/HCI 시스템에 대한 지능적이고 자동화된 지원이 중단되었습니다.

- **참고: 직접 연결을 활용하는 Dell PowerStore 및 Unity 제품을 보유한 고객의 경우** 해당 기술은 2024년 12월 31일에 서비스가 중단되었습니다. 서비스 중단을 방지하기 위해 EOSL(End of Service Life) 전에 운영 환경 업데이트가 제공됩니다.

SupportAssist Enterprise 4.x 및 2.x는 2022년 7월 31일에 서비스가 중단되었습니다. Dell 서버, 스토리지, 네트워킹 및/또는 CI/HCI 시스템에 대한 지능적이고 자동화된 지원이 중단되었습니다.

4: 고객이 설치하고 업그레이드할 수 있는 소프트웨어입니까?

예. Dell Technologies의 도움 없이 연결 기술을 다운로드하고 설치할 수 있습니다.

게이트웨이 및 플러그인 소프트웨어 리소스는 Dell 지원 사이트에서 참조할 수 있습니다.

- **팁:** 인터랙티브 기술 데모(영어로만 제공)를 통해 게이트웨이 에디션과 정책 관리자 소프트웨어의 설치, 등록 및 사용 방법을 미리 볼 수 있습니다.
- **팁:** 서비스 연결 준비 템플릿을 사용하여 Dell 지원 문서 자료에서 세부 정보를 빠르게 추출하여 네트워크를 연결할 준비를 하십시오. *Q15을 참조하십시오.*

5: 라이선스가 필요합니까?

소프트웨어 라이선스는 필요하지 않습니다. 단, 소프트웨어를 다운로드하고 등록하려면 Dell.com/Support에서 인증받아야 합니다.

기술의 특징 및 가치

6: 연결 소프트웨어를 사용하면 어떻게 Dell 지원 경험에서 더 많은 가치를 얻게 됩니까?

기업이 Dell Technologies의 연결 툴을 사용하는 주된 이유는 운영 환경의 다운타임을 줄이고, 중요한 문제를 모니터링해야 하는 부담을 줄이며, 작은 문제가 많은 비용을 초래하는 더 큰 문제로 발전하기 전에 이를 식별 및 해결하기 위해서입니다.

연결을 설정하면 지원 서비스가 적용되는 Dell 인프라스트럭처 제품에 대한 지원 경험이 향상됩니다 (예: ProSupport Infrastructure Suite의 모든 서비스 수준). 게이트웨이, 직접 연결 또는 플러그인 옵션으로 구현된 Secure Connect Gateway 기술이 현재 운영 환경에서 이러한 시스템을 모니터링하면 Dell Technologies는 선제적이고 사전 예방적이며 때로는 예측적인 지원을 제공합니다.

데이터는 Dell Technologies 연결 기술의 핵심입니다. **Dell Technologies는 고객 환경의 시스템 상태 데이터를 활용합니다.** 그리고 현장 및 기술 지원 팀과 구성 요소 제조업체에서 **수년간 수집된 인시던트 및 엔지니어링 데이터와 이 데이터의 상관관계를 분석합니다**. **머신 러닝을 비롯한 정교한 AI 모델**을 활용하여 Dell Technologies의 연결 기술은 텔레메트리 및 이벤트 데이터의 패턴을 찾아 적용함으로써 조치를 취할 적절한 문제를 정확하게 탐지할 수 있습니다.

Dell Technologies의 기술은 하드웨어 및 소프트웨어 문제를 파악하고, **케이스를 생성하여 저희에게 연락을 취해 문제가 심각한 문제로 발전하기 전에 해결을 시작합니다.** 문제 유형에 따라 알림을 통해 **자동 부품 발송을 시작**할 수도 있으며, 이를 통해 하드웨어 부품을 더 빨리 수령할 수 있습니다.

또 다른 유용한 기능은 **원격 지원**으로, 이는 대부분의 스토리지, 데이터 보호, 컨버지드 및 하이퍼컨버지드(CI/HCI) 제품에 포함되어 있습니다. 이러한 상황에서, 즉 저희 측에서 케이스가 개설되었을 때 원격 지원을 통해 문제를 해결할 수 있다면, 이 기술은 공인 기술 지원 에이전트가 관리되는 디바이스에 원격으로 액세스하여 문제를 진단하고 해결할 수 있는 안전한 양방향 통신을 지원합니다.

또한, 텔레메트리를 Dell로 다시 전송함으로써, Dell 지원 팀이 개입할 때 **시스템의 과거 데이터를 활용하여 문제 해결 시간을 단축할 수 있습니다**. 예를 들어, Dell로 알림이 다시 전송되면 기술 지원 담당자는 고객이 설정한 정책에 따라 디바이스에 연결한 다음 취해야 할 조치를 확인하고 고객에게 실행 계획을 제공할 수 있습니다. 예를 들어, 부품이 실제로 고장 나기 전에 교체하여 궁극적으로 다운타임 위험을 최소화할 수 있습니다.

원격 지원 기능의 또 다른 이점은 **원격 업그레이드**입니다. 이는 보안 연결을 어떻게 활용하는지 보여주는 좋은 예입니다. 많은 제품에는 고객이 편리하게 적용할 수 있도록 직접 발송된 제품에 대한 업그레이드 코드 또는 보안 패치가 있을 수 있습니다. 또는 원격 변경 관리 팀이 현장에 나가지 않고도 업그레이드를 예약하고 처음부터 끝까지 실행할 수 있습니다.

전문가의 견해 참조:

- 팟캐스트 청취(영어로만 제공): 지능형 지원으로 데이터 센터 가동 시간 극대화
- 팟캐스트 청취(영어로만 제공): 사전 예방적이고 예측적인 지원으로 PowerEdge 가동 시간 극대화

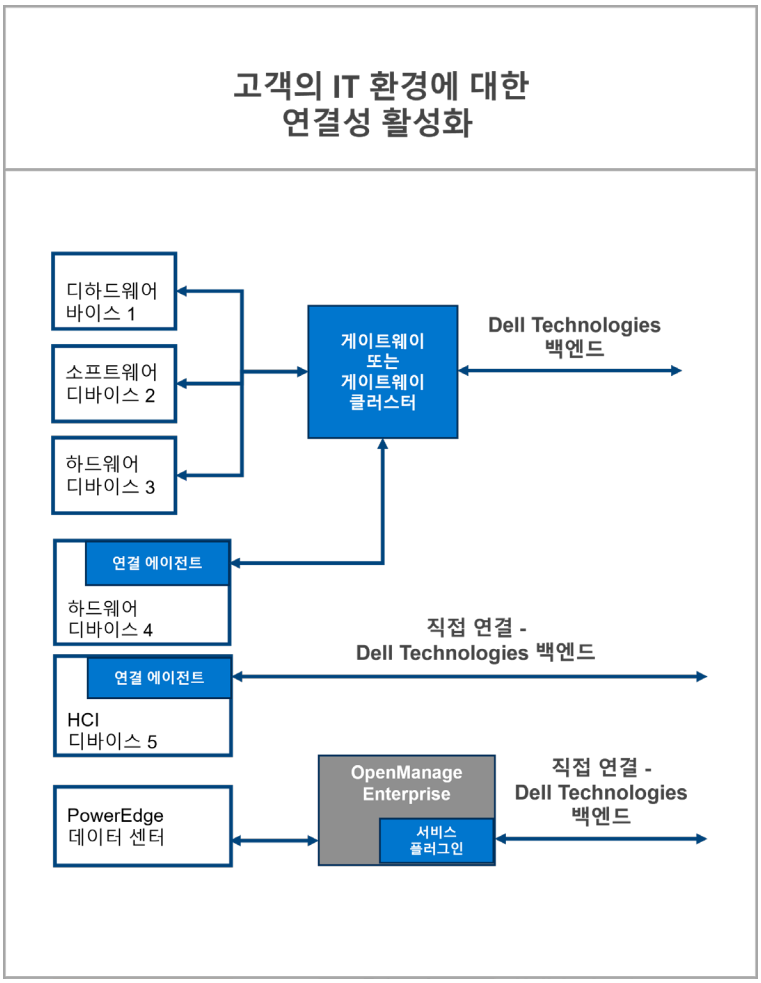
짧은 비디오 보기(영어로만 제공)**:**

- 연결 기능 및 이점
- 보안 아키텍처 및 기능

기술 배포 옵션

7: 현재 운영 환경에서 연결 소프트웨어를 배포하고 구성하는 방법에는 어떤 것들이 있습니까?

게이트웨이 옵션, 직접 연결 옵션, 플러그인 옵션 등 현재 운영 환경에 적합한 설치 옵션을 유연하게 선택할 수 있습니다. 이러한 옵션은 모두 고객이 설치하고 업그레이드할 수 있습니다.



보안 연결 **게이트웨이 옵션**을 사용하면 Dell 시스템을 게이트웨이에 연결하여 Dell Technologies Services와 다시 통신할 수 있습니다. 이를 통해 방화벽/네트워킹 설정이 간소화되어 게이트웨이만 인터넷을 통해 아웃바운드로 연결됩니다.

게이트웨이 옵션으로 Dell에서는 VMware, Microsoft Hyper-V 및 Linux KVM 환경을 위한 **가상 에디션**을 제공합니다. 또한 Docker, Podman, Kubernetes 및 OpenShift 환경을 위한 **컨테이너 에디션**도 제공합니다. 소규모 서버 고객을 위해서는 Windows/Linux 버전이 포함된 **애플리케이션 에디션**을 제공합니다. *Q8-11을 참조하십시오.*

시스템의 고가용성과 페일오버 기능을 원하는 고객은 게이트웨이를 여러 개 설정하거나, 게이트웨이 중 하나를 사용할 수 없는 경우 이중화 기능을 제공하는 클러스터를 설정할 수 있습니다.

직접 연결 옵션(Dell의 연결 기술을 Dell 제품의 운영 환경에 통합하여 지원)은 추가 소프트웨어 설치를 원치 않는 소규모 고객과 비기존 고객을 위한 옵션입니다. *자세한 내용은 Q12 및 Q29을 참조하십시오.*

마지막으로, 컴퓨팅 중심 고객을 위해서는 PowerEdge 서버 제품군에 **OpenManage Enterprise용 서비스 플러그인**을 제공하므로 안전한 단일 직접 연결을 구성할 수 있습니다. *자세한 내용은 Q13 및 Q24-28을 참조하십시오.*

주요 링크가 포함된 인포그래픽:데이터 센터에서 연결 시작하기

7 계속: 현재 운영 환경에서 연결 소프트웨어를 배포하고 구성하는 방법에는 어떤 것들이 있습니까?

아래 표를 사용하여 현재 운영 환경에 적합한 옵션을 알아보십시오. Secure Connect Gateway에 대한 제품 Support Matrix를 확인하거나, Dell.com/Support에서 하드웨어 제품 지원 페이지를 방문해야 합니다. 애플리케이션 버전은 가상화된 환경이 없고 지원되는 Dell 하드웨어 및 소프트웨어를 사용하는 소규모 고객에게 가장 적합합니다.

연결하여 한 곳에서 모든 디바이스를 모니터링

	통합 솔루션	지원되는 하드웨어 및 소프트웨어
통합 솔루션	**Secure Connect Gateway 5.x** **- Virtual Appliance 에디션** *VMware, Microsoft HyperV 및 Linux KVM 환경용 컨테이너 패키지: Docker, Podman, Kubernetes, OpenShift*	모든 Dell 제품 포트폴리오 - 데이터 스토리지, 서버, 네트워킹, CI/HCI 및 데이터 보호
	Secure Connect Gateway 5.x **– 애플리케이션 에디션** *서버에서 Windows Enterprise 관리* *서버에서 Linux 관리*	PowerEdge, iDRAC, PowerSwitch, Webscale, PeerStorage, EqualLogic, Compellent, Fluid File System(FluidFS), PowerVault
	OpenManage Enterprise Services plug-in *OpenManage Enterprise 환경 지원*	PowerEdge 서버
특정 Dell 하드웨어에 직접 연결	• Dell 제품 운영 환경으로 연결 통합. Dell 제품 지원 문서 자료를 참조하여 특정 제품 모델 및 버전을 확인하십시오. • 여러 Dell 하드웨어 제품의 이기종 구축에 적합. • Dell Technologies에 직접 연결하거나 Secure Connect Gateway 서버를 통해 연결	

주요 링크가 포함된 인포그래픽:데이터 센터에서 연결 시작하기

8: 현재 운영 환경에 권장되는 게이트웨이 소프트웨어와 최소 요구 사항은 무엇입니까?

게이트웨이 소프트웨어	
보안 연결 게이트웨이 - 가상 에디션 다음에 적합한 버전이 있습니다. • VMware, Microsoft HyperV 및 Linux KVM 환경 • 컨테이너 패키지: Docker, Podman, Kubernetes, OpenShift Dell.com/Support에서 설명서와 모든 리소스를 다운로드하십시오.	보안 연결 게이트웨이 - 애플리케이션 에디션 다음에 적합한 버전이 있습니다. • Windows 관리 서버(Windows 및 Linux 디바이스를 모두 모니터링) • Linux 관리 서버(Linux 디바이스 모니터링) Dell.com/Support에서 설명서와 모든 리소스를 다운로드하십시오.
인터랙티브 기술 데모를 미리 보고 설치, 등록 및 사용에 대한 기술 팁을 참조하십시오.	
보안 연결 게이트웨이 소프트웨어를 설치하고 사용하기 위한 최소 요구 사항을 확인하십시오.	

고객 연결을 위한 4단계

1. **사이트 준비 및 계정 확인**
   기술 요구 사항을 미리 보고 네트워크 관리자와 함께 계획합니다. 2단계 이전에 Dell.com/Support에서 엔터프라이즈 비즈니스 계정을 설정합니다.
2. **다운로드**
   Dell.com/Support의 Secure Connect Gateway에 대한 제품 지원 페이지에서 계정 자격 증명으로 로그인합니다.
   환경에 적합한 에디션을 다운로드하고 인증 액세스 키를 생성합니다.
3. **설치 및 프로비저닝**
   가상 어플라이언스 또는 컨테이너 템플릿을 배포하거나 애플리케이션 소프트웨어를 설치합니다. 초기 등록 단계를 완료합니다.
4. **디바이스 연결**
   Dell 제품과 게이트웨이 서버 간의 통신을 구성하고 활성화합니다.

신규 사용자의 시작을 위한 팁:

- 신규 사용자는 먼저 Dell.com/Support에서 엔터프라이즈 비즈니스 계정을 설정해야 합니다. Secure Connect Gateway 다운로드 페이지에서 로그인하고 이 단계를 완료하라는 메시지가 표시됩니다.
- 완료되면 Dell.com/Support의 Secure Connect Gateway 제품 지원 페이지에서 계정 자격 증명을 사용하여 로그인합니다.
- 소프트웨어 설치를 위한 사이트 위치를 반드시 입력하십시오. 그러면 Dell Technologies에서 더 나은 지원 경험을 제공할 수 있습니다.
- 현재 운영 환경에 적합한 에디션을 구매하십시오. 이 단계에서는 인증 액세스 키를 생성해야 합니다.

참고: *처음 연결하는 경우 사이트 준비에 가장 많은 시간이 소요됩니다. 네트워크 및 보안 정책의 복잡성에 따라 며칠에서 몇 달까지 걸릴 수 있습니다. 보안 및 네트워킹 팀에서 구현 전에 제품 검토를 요청할 수 있습니다.* 보안 문서를 확인하십시오.

기술 살펴보기: Dell.com을 방문하여 전문가의 견해 및 기술 리소스 참조하십시오.

도움이 필요하십니까? Secure Connect Gateway 포럼에서 Dell Technologies 전문가에게 무엇이든 물어보십시오.

9: 보안 연결 게이트웨이 디바이스를 Dell Technologies에 등록해야 합니까?

예. Secure Connect Gateway를 사용하고 동급 최고 수준의 보안을 보장받으려면 Dell Technologies에 등록해야 합니다.

> **팁:** 엔터프라이즈 비즈니스 계정 설정 방법을 알아보십시오. Dell.com/Support 에서 이름 옆에 검은색 확인 표시가 나타나면 올바르게 인증된 것입니다.

엔터프라이즈 비즈니스 계정을 사용하여 다운로드 페이지에 로그인하고 액세스 키와 PIN을 생성한 다음 액세스 키와 PIN을 사용하여 보안 연결 게이트웨이를 활성화합니다.

비즈니스 계정이 없는 고객은 소속 조직 및 제품에 대한 추가 정보를 요청받게 됩니다. 이러한 고객은 확인 절차를 거친 후 계속 진행할 수 있습니다.

10: 원격 지원 기능이 있는 게이트웨이 기술은 무엇입니까? 그리고 Secure Connect Gateway에서 관리하는 원격 액세스 기능이 탑재된 제품은 무엇입니까?

원격 지원 기능은 Secure Connect Gateway의 가상 에디션과 컨테이너 에디션에서만 사용할 수 있고, *애플리케이션 에디션에서는 사용할 수 없습니다*.

데이터 스토리지, 데이터 보호, 컨버지드 및 하이퍼 컨버지드(CI/HCI) 제품에는 원격 액세스 기능이 있습니다. PowerEdge 및 PowerSwitch 제품은 온프레미스 게이트웨이 관리 사용자 인터페이스의 디바이스 개요를 통해 원격 지원을 활성화할 수도 있습니다.

공인 기술 지원 에이전트는 필수 2단계 인증을 사용하여 관리되는 디바이스에 원격으로 액세스하여 문제를 해결합니다. 모든 원격 세션은 감사를 거치며, 세부 정보는 Secure Connect Gateway의 온프레미스 게이트웨이 관리 콘솔의 감사 섹션에서 확인할 수 있습니다.

추가 제어 및 고급 감사 기능을 위해, 고객은 유연하게 모든 원격 액세스 세션을 차단하거나 허용할 수 있는 정책 관리 서버를 설정할 수 있습니다.

11: 정책 관리자 소프트웨어란 무엇이며 게이트웨이 옵션에 어떻게 사용됩니까?

보안 연결 게이트웨이용 정책 관리자는 고급 감사 및 원격 제어 기능을 위해 설치할 수 있는 별도의 보완 외부 소프트웨어입니다.

정책 관리자를 사용하면 이러한 원격 액세스 기능 중 하나 이상을 지원하는 제품의 원격 지원, 파일 전송 또는 원격 작업에 대한 정책을 설정할 수 있습니다.

참고: *정책 관리자는 게이트웨이의 가상 에디션과 컨테이너 에디션에서만 사용할 수 있습니다. 애플리케이션 에디션에서는 사용할 수 없습니다.*

> **팁:** 인터랙티브 데모에서 정책 관리 모듈을 미리 살펴보십시오. Virtual Appliance 에디션의 기술 사용 방법 비디오를 확인하십시오.

12: 직접 연결이 가능한 제품은 무엇입니까? 게이트웨이와도 직접 연결을 사용할 수 있습니까?

경우에 따라 Dell Technologies의 연결 기술은 Dell 제품의 운영 환경에 통합되어 Dell Technologies Services 백엔드에 직접 연결할 수 있습니다. 이것이 바로 '직접 연결'을 의미합니다.

Dell 하드웨어 및 소프트웨어 제품을 설정하는 중에 연결 서비스를 활성화하라는 메시지가 표시됩니다.

하지만 언제든지 직접 연결이 활성화된 Dell 제품을 게이트웨이를 통해 연결하도록 전환할 수 있습니다. 회사의 보안 및 네트워킹 정책이 구성 결정에 영향을 미칩니다.

직접 연결이 활성화된 Dell 인프라스트럭처 제품 *항상 Dell.com/Support에서 지원 대상 제품의 최신 목록을 확인하십시오.*
AppSync | APEX AIOps Infrastructure Observability Collector | CMS – VxBlock 소프트웨어 데이터 백업/Avamar | Data Domain | Data Domain 관리 콘솔 | Edge Orchestrator Elastic Cloud Storage | Metro Node Appliances | ObjectScale PowerFlex 제품군 – 어플라이언스, 랙, 소프트웨어 PowerProtect - Data Manager, Data Manager 어플라이언스, 스케일 아웃 어플라이언스 PowerScale | PowerStore | PowerVault | S5000 Series | SRM | 데이터 스트리밍 | Unity | VxRail *직접 연결 기능이 포함된 특정 제품 모델 및 버전을 확인하려면 제품 지원 문서를 참조하십시오.*
PowerEdge: 서버의 직접 연결 옵션에 대한 업데이트는 *Q29를 참조*하십시오. *참고: 대상 디바이스에는 게이트웨이의 가상 어플라이언스 에디션을 통해서만 연결할 수 있는 옵션이 있습니다.*

참고: *SupportAssist, SupportAssist Enterprise 및 Secure Remote Services 소프트웨어 기능은 이제 차세대 연결 소프트웨어 플랫폼에 포함됩니다. 제품 사용자 인터페이스의 이러한 소프트웨어 참조는 향후 이에 따라 업데이트될 예정입니다.*

13: OpenManage Enterprise용 서비스 플러그인이란 무엇입니까?

Secure Connect Gateway 기술도 플러그인으로 구현되었습니다. PowerEdge 데이터 센터에서 OpenManage를 활용하는 고객의 경우, 이제 OpenManage Enterprise용 플러그인으로 연결하여 알림, 자동 디스패치 및 수집 기능을 사용할 수 있습니다. *Q25, 26, 28도 참조하십시오.*

리소스:

- 플러그인에 대해 자세히 알아보고 기술 리소스를 참조하십시오.
- 지원되는 제품은 OpenManage Enterprise Services 제품 지원 페이지에서 제품 Support Matrix 문서를 참조하십시오.

전문가의 견해 참조:

- **짧은 비디오 보기**(영어로만 제공)**:** OpenManage Enterprise용 서비스 플러그인
- **팟캐스트 청취**(영어로만 제공)**:** 사전 예방적이고 예측적인 지원으로 PowerEdge 가동 시간 극대화
- **읽기:** 보안 백서

14: 연결 소프트웨어 배포 지원을 받으려면 어떻게 합니까?

많은 고객이 Dell Technologies의 도움 없이 연결 기술을 다운로드하여 설치합니다. 웹 페이지에서 모든 리소스를 확인할 수 있습니다.

팁: 인터랙티브 기술 데모를 실행하고 탐색할 수 있습니다.

- *게이트웨이 에디션과 정책 관리자의 설치, 등록 및 사용 방법 미리 보기*

도움이 필요한 고객을 위해 ProDeploy Infrastructure Suite 서비스에는 보안 연결 게이트웨이의 사용 지원과 구성이 포함되어 있습니다.

ProSupport Plus 지원 서비스를 이용하는 고객에게는 설치 및 등록 관련 문의에 도움을 드릴 수 있는 Technical Customer Success Manager가 배정됩니다.

다른 고객은 필요에 따라 Dell Technologies 지원 부서에 도움을 요청해야 합니다.

15: 연결할 준비가 되었습니다. 시스템을 연결하기 전에 네트워킹 팀이 모든 정보를 정확하게 갖추고 있는지 어떻게 확인할 수 있습니까?

이 서비스 연결 준비: 네트워크 준비 템플릿을 사용하면 Dell 지원 문서 자료에서 최소 네트워크 요구 사항, 게이트웨이 및 디바이스별 포트 요구 사항, 방화벽 규칙 예외 세부 정보를 신속하게 추출하여 네트워크 연결 준비를 완료할 수 있습니다.

이 템플릿을 사용하여 게이트웨이, 직접 연결 및 플러그인 옵션으로 배포되는 Secure Connect Gateway 기술을 위한 네트워크 준비를 간소화할 수 있습니다. Dell 제품 및 IT 환경에 대한 질문에 답변하기만 하면 네트워크 요구 사항을 생성할 수 있습니다. 그런 다음 세부 정보를 즉시 사용 가능한 보고서로 다운로드하여 네트워킹 및 보안 팀과 공유합니다.

이 템플릿은 새로운 연결 설치 및 제품 연결 과정을 안내합니다. 기존 연결 구성 내에서 새 제품을 연결할 때도 적합합니다.

단계:

1. 서비스 연결 준비: 네트워크 준비 템플릿 링크를 클릭하여 zip 파일을 다운로드합니다. **참고:** 항상 이 링크에서 최신 템플릿을 다운로드하여 사용하십시오.
2. 새 폴더에 파일의 압축을 풀고 애플리케이션을 실행하여 템플릿을 엽니다.
3. 연결할 Dell 제품 및 IT 환경에 대한 질문에 답변하여 양식을 작성합니다.
4. 작성된 결과를 Excel 형식으로 저장하거나 내보내 네트워킹 및 보안 팀과 공유할 수 있습니다.

참고: 이 오프라인 템플릿은 Dell 지원 문서 자료를 최신 상태로 유지하기 위해 주기적으로 업데이트됩니다.

16: 문제가 발생하는 경우 지원 담당자에게 문의하려면 어떻게 해야 합니까?

Dell.com 온라인 지원 또는 Secure Connect Gateway 관련 문제가 발생하는 경우, 여기에서 관리 지원 페이지를 방문하여 도움을 요청하십시오. 문제와 가장 유사한 범주를 선택하고 안내에 따라 세부 사항을 입력하십시오. 기술 지원 문제에 대한 즉각적인 지원이 필요한 경우 여기에서 Dell Technologies에 문의하십시오. Technical Customer Success Manager에게 문의하십시오(해당하는 경우).

보안

17: 고객 환경에서 이 소프트웨어가 어떻게 작동하고 Dell과 어떻게 연결되는지 자세히 설명해 주십시오. 어떻게 보안이 유지됩니까?

현재 운영 환경과 Dell 간의 연결은 상호 TLS 터널 및 인증서 체인을 통해 보호됩니다. 이 유형의 구성에서는 시스템이 현재 운영 환경의 Dell 소프트웨어에 연결되며, 이러한 연결은 내부 포트/네트워킹 변경으로만 이루어집니다. 이 소프트웨어는 인터넷을 통해 아웃바운드로 연결하고 Dell로 다시 연결하는 유일한 수단입니다. 연결된 모든 시스템의 이벤트 및 텔레메트리 데이터를 수집하는 집계 지점 역할을 합니다. 이 정보는 전송되는 유일한 시스템 상태 정보입니다.

시스템의 모든 텔레메트리는 HTTPS TLS 1.3을 통해 전송됩니다. 또한 보안 터널을 사용하여 시스템에 액세스하고 문제를 해결하는 원격 지원 기능을 제공하여 문제 해결 속도를 높이고 다운타임을 방지합니다.

보안 문서에서 자세히 알아보십시오.

18: 원격 지원은 어떻게 수행됩니까? 누가 원격 지원 세션을 통해 Dell에서 시스템에 액세스할 수 있습니까?

Dell Technologies의 기술 지원 엔지니어는 포털을 사용하여 문제 해결 및 업그레이드 작업을 위해 시스템에 액세스할 수 있는 원격 지원 세션을 생성합니다. 다단계 인증을 사용하여 이 포털에 액세스합니다. 이러한 Dell 팀원은 엄격한 교육을 이수해야 하며, 액세스하려면 경영진의 승인을 받아야 합니다. Dell Technologies는 엔터프라이즈 연결 시스템에 널리 사용되는 솔루션인 MQTT 프로토콜을 원격 지원 에이전트로 사용합니다.

19: 이 시스템 상태 데이터 이벤트와 텔레메트리 정보는 보안을 중심으로 감사되고 있습니까? 정책 관리자의 역할은 무엇입니까?

Dell Technologies는 모든 거래를 감사하며, 소프트웨어의 사용자 인터페이스에서 이 정보를 확인하실 수 있습니다. 모든 원격 지원 세션, 이벤트 및 텔레메트리 전송을 확인하실 수 있습니다.

더욱 엄격한 보안 정책을 적용하거나 이 정보를 장기간 보관해야 하는 타사 감사 기관을 이용하는 고객의 경우, 정책 관리자 소프트웨어 설치를 권장합니다. Dell의 정책 관리자는 Secure Connect Gateway와 연동하여 고급 감사 및 원격 지원 제어 기능을 제공합니다. *Q11도 참조하십시오.*

20: 연결 기술의 보안 아키텍처에 대한 자세한 정보는 어디에서 확인할 수 있습니까?

보안 연결 게이트웨이 기술이 데이터 보호 및 위협 방지를 안전하고 자동화된 지원 환경에 통합하는 방법을 알아보려면 보안 백서를 다운로드하십시오.

이 백서에서 다루는 내용은 다음과 같습니다.

- **안전한 현장 데이터 수집:** 보안 연결 게이트웨이로 고객이 인증 요구 사항을 제어하고 2단계 인증 프로토콜을 활용하도록 지원하는 안전한 통신 브로커 역할을 수행하는 방법에 대해 알아봅니다.
- **안전한 데이터 전송 및 통신:** 보안 연결 게이트웨이가 암호화 및 상호 인증을 사용하여 하트비트 폴링, 원격 알림 및 원격 액세스 기능을 제공하는 안전한 TLS(Transport Layer Security) 터널을 생성하는 방법에 대해 알아봅니다.
- **안전한 데이터 저장, 사용 및 처리:** 물리적 보안, 공급망 위험 관리 및 안전한 개발 프로세스를 비롯하여 데이터를 보호하기 위해 구현된 다양한 수단에 대한 자세한 내용을 알아봅니다.

전문가의 견해 참조:

- **팟캐스트 청취**(영어로만 제공)**:** 지능형 지원으로 데이터 센터 가동 시간 극대화
- **읽기:** 보안 백서

짧은 비디오 보기(영어로만 제공)**:**

- 보안 아키텍처 및 기능
- 대규모 환경과 소규모 환경을 위한 보안 구성
- 금융 부문을 위한 보안 기능

또는 웨비나 시청(영어로만 제공)**:** Spiceworks Community 이벤트에서 다음에 대한 전문가의 이야기를 들어보십시오.

- 보안 연결 게이트웨이가 개인 정보 보호, 데이터 보호 및 위협 방지를 통합하는 방법
- 소규모, 대규모 및 기존과 다른 환경 전반에 걸쳐 연결을 유연하게 구축하는 방법
- 자동화된 지원이 연결된 시스템의 문제를 예방하고 완화하는 데 도움이 되는 이유

구성 시나리오

21: 회사의 요구 사항에 맞게 연결 기술을 배포하고 구성하기 위한 고려 사항에는 어떤 것들이 있습니까?

가장 먼저 고려해야 할 항목은 연결을 위해 구성할 **제품 유형(컴퓨팅, 스토리지, 데이터 보호, 컨버지드 및 하이퍼 컨버지드(CI/HCI))**과 다음과 같은 **현재 운영 환경**입니다.

- 데이터 센터들이 네트워크로 한데 연결되어 있습니까?
- 컴퓨팅 또는 스토리지(데이터 보호, CI/HCI 제품 포함)를 *별도로 관리합니까, 아니면 통합하여 관리합니까*?

회사의 **보안 및 네트워킹 정책**도 고려해야 합니다. 또한, **팀이 모든 제품을 함께 관리하기를 원하는지 또는 지리적 위치나 제품 유형별로 분류하기를 원하는지**도 고려해야 합니다.

근본적으로 사물이 어떻게 연결되는지, 팀이 어떻게 협력하는지, 네트워크 복잡성을 최소화하는 방법이 무엇인지 생각해야 합니다. 그렇게 하면 다양한 배포 옵션을 기반으로 가장 효과적인 아키텍처를 설계할 수 있습니다.

이에 대해 설명하는 **연결 구성 고려 사항** 개요를 **읽고 공유하십시오.**

1. 보안에 민감한 대규모 회사에 권장되는 구성은 무엇입니까?
2. 중간 규모 조직과 소규모 조직에 적합한 구성 및 구축 옵션은 무엇입니까?
3. 컴퓨팅 중심 환경을 갖춘 대기업 및 중견 기업의 경우 어떻게 해야 합니까? 어떤 툴을 사용할지 어떻게 결정합니까?
4. 1~50대의 PowerEdge 서버가 있고 가상화된 환경이 없는 경우 어떻게 해야 합니까? 게이트웨이 옵션에는 어떤 것들이 있습니까?
5. 직접 연결이 가능한 Dell 제품이 있는 경우 어떻게 해야 합니까? 일반적인 활용 사례에는 어떤 것이 있습니까?
6. 우리 회사에 적합한 구성은 무엇입니까?

팁: 서비스 연결 준비 템플릿을 다운로드하고 사용해서 네트워크 설정을 위한 특정 포트 및 방화벽 요구 사항이 포함된 보고서를 네트워킹 및 보안 팀을 위해 생성하십시오. ***Q15을 참조하십시오.***

지원 서비스

22: 연결은 Dell 인프라스트럭처 제품에 대한 지원 서비스 계약의 가치와 어떤 관련이 있습니까?

간단히 말해, 현재 운영 환경에 연결 소프트웨어를 배포하고 이 소프트웨어로 모니터링할 Dell 디바이스를 연결하면, Dell 시스템에 대한 활성 지원 계약을 통해 더 큰 가치를 얻을 수 있습니다. 무료 소프트웨어로, 라이선스가 필요하지 않습니다. 90개 이상의 Dell 인프라스트럭처 제품(하드웨어 및 소프트웨어)을 지원합니다. 더 스마트한 AI, 자동화된 지원 및 실시간 분석의 고유한 통합 기능을 통해 이점을 누릴 수 있습니다.

ProSupport Infrastructure Suite 서비스를 이용하는 고객은 모든 수준에서 큰 가치를 얻을 수 있습니다.

- 자세한 정보: Dell 인프라스트럭처 시스템에 대한 ProSupport 및 ProSupport Plus 적용
    - 자세한 정보: Lifecycle Extension with ProSupport 또는 ProSupport Plus
- 참고: Basic Hardware Support(영업일 기준 익일)가 적용되는 Dell 시스템의 경우 연결 소프트웨어로 모니터링할 때 자동화된 문제 탐지, 케이스 생성 및 알림 기능의 이점도 얻을 수 있습니다. 문제가 탐지되면 기본 지원 고객은 케이스 번호가 포함된 이메일을 받고, 문제 해결 및 해결에 대한 Dell 지원을 원한다는 것을 확인하기 위해 적시에 Dell 지원 팀으로 연락하라는 메시지를 받게 됩니다.

인프라스트럭처용 특별 지원 서비스도 살펴보십시오.

23: 모니터링 대상 시스템의 ProSupport Infrastructure Suite와 같은 지원 서비스 계약의 적용이 만료될 경우 자동화된 지원 기능은 어떻게 됩니까?

모든 수준의 ProSupport Infrastructure Suite에 대한 서비스 계약이 만료되면 자동 케이스 생성 기능이 비활성화됩니다. 하지만 게이트웨이, 직접 연결 또는 플러그인으로 배포된 Secure Connect Gateway 기술은 자동화된 시스템 상태 수집을 계속 실행합니다. 시스템(서비스 태그)에서 계약을 업그레이드하거나 연장하는 경우, 해당 시스템에서 자동 케이스 생성이 자동으로 다시 활성화됩니다.

PowerEdge 연결

24: 서버에 이 연결 소프트웨어를 배포하고 구성하는 가장 좋은 방법은 무엇입니까? 어떤 툴을 사용할지 어떻게 결정합니까?

간단히 말해서, OpenManage Enterprise를 통한 서비스 플러그인 솔루션은 컴퓨팅 중심 환경을 사용하는 고객에게 적합하며, 게이트웨이 솔루션은 다양한 Dell 인프라스트럭처 제품을 관리하는 데 적합한 옵션입니다.

두 솔루션 모두 지원 계약을 체결한 PowerEdge 서버에 대한 알림, 자동 케이스 생성, 자동 디스패치 및 텔레메트리 수집 기능을 포함합니다.

고객이 선택해야 하는 솔루션은 현재 사용 중인 환경 유형, 환경 간의 네트워킹, 모니터링 대상 디바이스 유형 및 기본 설정에 따라 달라집니다.

OpenManage Enterprise를 이미 설치했거나 설치를 고려 중이라면 서비스 플러그인이 적합합니다! OpenManage Enterprise는 단일 콘솔에서 PowerEdge 서버 수천 대의 수명주기 관리를 용이하게 하는 Dell의 인프라스트럭처 솔루션입니다.

- 이 솔루션을 처음 사용하는 경우, 현재 운영 환경에 Open Manage Enterprise를 설치하고 서버 제품을 온보딩한 다음 방화벽이 올바르게 구성되어 있는지 확인한 후 서비스 플러그인을 설치하면 됩니다. 그러면 알림과 텔레메트리가 Dell로 전송되기 시작합니다.

PowerEdge와 함께 실행되는 PowerStore, PowerMax, PowerScale, Data Domain, VxRail 등의 Dell 인프라스트럭처 제품 조합을 사용하는 고객의 경우 단일 UI에서 이러한 시스템을 관리하기 위한 보안 연결 게이트웨이 솔루션을 설치하는 것이 좋습니다.

전문가의 견해 참조:

- **팟캐스트 청취**(영어로만 제공)**:** 사전 예방적이고 예측적인 지원으로 PowerEdge 가동 시간 극대화
  - OpenManage Enterprise 솔루션을 통한 PowerEdge 시스템 연결에 필요한 구성 요소 및 게이트웨이 솔루션을 통한 연결과의 차이점
  - PowerEdge 디바이스 자체에 연결하는 방법
  - 시기에 따라 연결된 서버 수를 쉽게 확장하는 방법
  - 기타 구성 시나리오: 플러그인 옵션과 게이트웨이 옵션을 모두 실행

서버 직접 연결 옵션 업데이트

- 제품 및 지역별 세부 정보와 연결 고려 사항에 대한 지침을 포함한 모든 세부 정보는 *Q29을 참조*하십시오.

25: 서비스 연결이 OpenManage Enterprise의 데이터 센터 관리 수명주기 모니터링 기능을 어떻게 보완합니까?

OpenManage Enterprise는 사용이 간편한 일대다 시스템 관리 콘솔입니다. 하나의 콘솔에서 PowerEdge 서버 및 섀시에 대한 포괄적인 수명주기 관리를 비용 효율적으로 지원합니다.

아래 다이어그램을 통해 OpenManage Enterprise용 연결 플러그인이 데이터 센터의 OpenManage Enterprise 경험을 어떻게 보완하는지 확인하십시오.

이 기능은 현재 **OpenManage Enterprise용 서비스 플러그인**을 통해 사용할 수 있습니다. 이 플러그인을 통해 Secure Connect Gateway 기술의 사전 예방적이고 예측적인 지원 기능을 사용할 수 있으며 PowerEdge 서버를 단일 OpenManage Enterprise 콘솔에서 관리할 수 있습니다. 자세히 알아보고 관련 리소스를 찾아보십시오.

26: OpenManage Enterprise용 서비스 플러그인은 어떤 시스템을 지원합니까?

iDRAC 및 CMC(Chassis Management Controller)를 사용하는 PowerEdge 서버 및 섀시와 Linux 서버를 지원합니다.

지원되는 제품을 구체적으로 확인하려면 Dell.com/Support 사이트를 방문하여 OpenManage Enterprise Services 제품 지원 페이지에서 Support Matrix 문서를 참조하십시오.

27: 서비스용 연결 소프트웨어를 사용하면 OpenManage Enterprise와 유사하게 PowerEdge 서버에 대한 데이터 센터 수명주기 관리 작업을 수행할 수 있습니까?

아니요. 서비스용 연결 소프트웨어는 데이터 센터의 독립 실행형 PowerEdge 디바이스에 대한 BIOS 및 펌웨어 업데이트를 전송하거나 오케스트레이션하지 *않습니다*. 일반적으로 독립 실행형 서버 환경을 사용하는 컴퓨팅 중심 고객은 이러한 유형의 수명주기 관리 기능을 위해 OpenManage Enterprise를 설치하여 사용합니다.

참고: OpenManage Enterprise용 서비스 플러그인을 활성화하면 활성 지원 계약이 있는 PowerEdge 서버에 대한 알림, 자동 케이스 생성, 자동 디스패치 및 텔레메트리 수집 기능이 활성화됩니다. 그러나 서비스 플러그인은 관리 대상 시스템에 대한 업그레이드 코드 제공 및 원격 지원 액세스 기능을 활성화하지 *않습니다*.

28: OpenManage Enterprise 환경에서 서비스 플러그인과 AIOps 플러그인은 언제 사용해야 합니까? AIOps 플러그인을 사용하면 자동화된 사전 예방적 지원 케이스 생성 기능을 사용할 수 있습니까?

OpenManage Enterprise는 단일 콘솔에서 PowerEdge 서버 수천 대의 수명주기 관리를 용이하게 하는 Dell의 인프라스트럭처 솔루션입니다. 아래 표에서 서비스 플러그인과 AIOps 플러그인의 사용 및 기능을 비교해서 설명합니다.

OpenManage Enterprise 콘솔에서 서비스 플러그인과 AIOps 플러그인을 *모두* 활성화하여 각각의 기능을 최대한 활용하는 것이 좋습니다.

기능 및 활용 사례 개요		
플러그인	OpenManage Enterprise **서비스 플러그인**	OpenManage Enterprise **AIOps 플러그인**
사용하려는 시기는?	**자동화된 사전 예방적 지원 기능**을 원할 때 활성화	**Dell AIOps 클라우드 기반 대시보드의 기능**을 원할 때 활성화
플러그인 기능	알림, 자동 케이스 생성, 부품 자동 디스패치 및 텔레메트리 수집 기능 제공	용량 부족, 성능 이상 징후, 사이버 보안 위험 및 지속 가능성에 대한 상태 모니터링 및 예측 통찰력 제공
기능 활성화 대상	ProSupport 및 ProSupport Plus 계약을 포함한 활성 지원 계약이 있는 자산. *Q21을 참조하십시오.*	ProSupport 및 ProSupport Plus 계약이 있는 자산
보안 연결 설정 설명	참고: 고객은 운영 환경에서 두 개가 아닌 하나의 연결을 활성화합니다. 고객 운영 환경의 OpenManage 어플라이언스와 Dell 백엔드 *간에는* Secure Connect Gateway 기술을 기반으로 한 하나의 보안 상호 TLS 연결이 설정됩니다.	
핵심 요점	서비스 플러그인만 활성화하면 AIOps 플러그인 기능을 사용할 수 없습니다. AIOps 플러그인만 활성화하면 서비스 플러그인 기능을 사용할 수 없습니다. **모범 사례 권장 사항: 두 플러그인을 모두 활성화합니다.**	

29: 일부 PowerEdge 시스템에 나타나는 Dell Connectivity Client는 무엇입니까? Secure Connect Gateway 기술과 호환됩니까? Dell AIOps와 호환됩니까?

iDRAC과 함께 제공되는 특정 PowerEdge 서버 모델에는 Dell Connectivity Client라는 iDRAC(integrated Dell Remote Access Controller) 플러그인이 포함되어 있습니다. 제품 및 지역별 세부 정보는 FAQ를 참조하십시오. 이 클라이언트는 iDRAC에서 Dell 백엔드 서비스로의 직접 연결을 활성화하고, OpenTelemetry 프레임워크를 사용하여 스트리밍 텔레메트리를 제공합니다.

- **참고**: 이 PowerEdge 제품 구성은 Dell에서 사전 활성화하므로 고객은 영업 프로세스 중에 Dell Connectivity Client 사용을 명시적으로 동의/거부해야 합니다.

Secure Connect Gateway 기술과의 호환성:

Dell Connectivity Client는 v5.32부터 Secure Connect Gateway의 가상 어플라이언스 에디션을 통해 연결하도록 전환할 수 있습니다. 고객은 스트리밍 텔레메트리를 위해 Dell에 대한 연결을 설정하려면 게이트웨이 내에서 '*Streaming Telemetry Connection*'을 명시적으로 선택해야 합니다.

- **참고:** 게이트웨이의 온프레미스 감사 및 수집 기능은 이 클라이언트를 통해 연결하는 iDRAC 모델에서 지원되지 않습니다. 또한 게이트웨이의 디바이스 상태 세부 정보가 제한되며 IPv6는 지원되지 않습니다.

고객이 거부하면 이러한 iDRAC 모델은 Dell Connectivity Client를 통한 연결 대신 기존 게이트웨이 연결을 사용합니다. 따라서 스트리밍 텔레메트리가 활성화되지 않습니다.

현재 Dell Connectivity Client는 Secure Connect Gateway의 컨테이너 또는 애플리케이션 에디션이나 OpenManage Enterprise용 서비스 플러그인에 연결할 수 없습니다.

모범 사례 권장 사항:

현재 운영 환경에서 PowerEdge 시스템에 대해 Secure Connect Gateway 또는 서비스 플러그인을 이미 사용 중인 경우:

- 이러한 기존 구성을 계속 사용할 수 있으며 Dell Connectivity Client를 통해 해당 PowerEdge 시스템을 Dell에 다시 연결할 *필요가 없습니다*. 하지만 해당 PowerEdge 시스템에 대해 Dell Connectivity Client를 비활성화하는 *조치를 취해야 합니다*. Dell Connectivity Client 구성을 비활성화하는 방법에 대한 이 가이드를 참조하십시오.

게이트웨이 연결과 같은 보안 정책을 준수하기 위해 회사에 단일 보안 연결이 필요한 경우 다음을 권장합니다.

- Secure Connect Gateway 또는 OpenManage Enterprise용 서비스 플러그인에 적합한 버전의 가상, 컨테이너 또는 애플리케이션 에디션을 다운로드하여 설치합니다.
- 또한, 해당 PowerEdge 시스템에 대해 Dell Connectivity Client를 비활성화하는 조치를 취해야 합니다. 그런 다음 기술 가이드에 따라 모니터링을 위해 이러한 시스템을 게이트웨이에 연결하거나 OpenManage Enterprise를 통해 연결합니다. 이러한 기술 배포 옵션에 대해 자세히 알아보십시오.

Dell AIOps의 텔레메트리에 대한 참고 사항:

Dell Connectivity Client에 직접 연결하거나 스트리밍 텔레메트리 연결이 있는 게이트웨이를 통해 연결하는 iDRAC 모델의 경우 Dell AIOps 플랫폼에 텔레메트리를 제공하기 위해 추가 설정이 필요하지 않습니다.

그러나 고객은 Dell AIOps 대시보드에 액세스하고 이러한 모델을 온보딩하여 Dell AIOps 기능 및 통찰력을 활성화해야 합니다. 대시보드에 대한 액세스는 ProSupport 또는 ProSupport Plus for Infrastructure 서비스 및 ProSupport One for Data Center 서비스에 포함되어 있습니다. Q36도 참조하십시오.

기타 일반적인 정보

30: Secure Connect Gateway의 알림 정책에 대한 정보는 어디에서 찾을 수 있습니까? 하드웨어 장애에 대한 예측 지원 케이스는 언제 개설됩니까?

Dell Technologies의 Secure Connect Gateway 알림 정책은 Dell Technologies 기술 지원 팀에 케이스를 개설하는 알림에 대한 정보를 제공합니다. Secure Connect Gateway를 사용하는 고객은 ProSupport Plus 서비스가 제공되는 시스템의 서버 하드웨어(하드 디스크, 백플레인 및 확장기)에 대한 자동 예측 케이스 생성 기능만 이용할 수 있습니다. 예측 알림은 Dell Technologies에 제출되는 예약된 수집을 기반으로 합니다.

31: 게이트웨이의 자격 증명 관리 기능에 대해 알아야 할 사항은 무엇입니까?

Secure Connect Gateway는 여러 자격 증명 계정 및 프로파일을 추가할 수 있는 유연성을 제공합니다. 자격 증명 계정을 사용하면 관리자가 제품 유형별로 인증을 추가할 수 있습니다. 또한 프로파일을 사용하면 기능 또는 리전별로 다른 여러 관리자가 각자의 계정을 관리할 수 있습니다. 자격 증명이 필요한 제품으로는 PowerEdge 서버, iDRAC, Compellent, 네트워킹, PS Series, MD Series 및 Webscale 시스템이 있습니다.

Dell Technologies는 자격 증명 볼트 통합도 제공합니다. 이는 여러 디바이스를 사용하는 고객에게 매우 유용한 기능으로, 보안을 약화시키거나 수동 작업을 늘리지 않고도 시스템을 추가하고 올바른 자격 증명을 유지할 수 있습니다. Dell Technologies는 현재 CyberArk Conjur API 및 CyberArk Credential Provider 제품을 지원하는 시장 선도 기업인 CyberArk와 통합되어 있습니다. 또한 Microsoft Azure Key Vault 및 HashiCorp 자격 증명 볼트도 지원합니다. 더 많은 공급업체가 추가될 예정입니다. 최신 목록은 지원 문서 자료를 확인하십시오.

팁: 인터랙티브 데모의 *디바이스 관리* 모듈에서 이러한 기능을 미리 볼 수 있습니다.

32: 유지 보수 모드의 주요 기능은 무엇입니까?

하드웨어 알림이 빠르게 연속으로 발생하여 사전 정의된 횟수 제한을 위반하면 "이벤트 폭주"가 발생합니다. 이 경우, Secure Connect Gateway는 이벤트 폭주를 유발한 특정 디바이스에 대한 알림 처리를 중단합니다. 다른 모든 디바이스는 지원 케이스를 생성할 수 있는 검증된 알림을 위해 Secure Connect Gateway에서 계속 모니터링됩니다.

또한, 사용자는 시스템 내에서 하나 이상의 디바이스에 대한 유지 보수를 수동으로 활성화할 수 있습니다. 이 기능은 계획된 유지 보수에 사용할 수 있으며, Secure Connect Gateway가 해당 디바이스를 모니터링하지 않도록 하려는 경우에 배포할 수 있습니다. 계획된 유지 보수 작업이 완료되면 유지 보수 모드를 수동으로 비활성화하여 Secure Connect Gateway에 모니터링을 재개하도록 신호를 보낼 수 있습니다.

33: 이 게이트웨이 옵션은 이메일 알림 기본 설정을 설정하도록 지원합니까?

예. 이메일 알림 기본 설정은 Settings 탭의 Secure Connect Gateway 사용자 인터페이스에서 조정할 수 있습니다. 자세한 내용은 사용자 가이드를 참조하십시오.

34: 온프레미스 게이트웨이 관리 대시보드에서는 어떤 언어가 지원됩니까?

Secure Connect Gateway 소프트웨어 인터페이스는 영어, 독일어, 포르투갈어(브라질), 프랑스어, 스페인어, 중국어(간체) 및 일본어로 제공됩니다. 단, 고객은 서비스 요청 인시던트 시 전송되는 자동 이메일 알림에 대해 28개 언어 중 1개를 선택할 수 있습니다. 참고: 일부 이메일 알림은 OS 제한으로 인해 현지 언어로 번역되지 않습니다.

35: REST API를 시작하려면 어떻게 해야 합니까?

게이트웨이 옵션을 사용하면 고객이 REST API를 사용하여 자체 맞춤형 스크립팅을 수행하고 지원할 수 있습니다. REST API 사용자 가이드는 설명서 섹션에서 다운로드할 수 있습니다.

36: Dell AIOps 포털에서 이 연결 소프트웨어는 어떻게 사용됩니까?

Dell AIOps(이전 명칭: APEX AIOps Infrastructure Observability 및 CloudIQ)는 Dell 인프라스트럭처를 최적화하도록 설계된 클라우드 기반의 AI 기반 관찰 및 관리 솔루션입니다.

인프라스트럭처 성능을 극대화하고, 사이버 보안을 강화하며, 지속 가능성을 높이고, 사전 예방적 계획을 지원하는 실시간 통찰력을 제공합니다. 직관적인 플랫폼과 Generative AI Assistant를 제공하는 Dell AIOps는 위험을 최소화하고 효율성을 높이며 IT 운영을 간소화해줍니다.

- 주요 특징으로는 상태 및 사이버 보안 위험 진단 및 문제 해결을 위한 권장 사항, 성능 및 용량 추적, 이상 징후 탐지 및 예측, 실패 예측, 에너지 및 배출 추적 및 예측, 가상화 리소스 모니터링 등이 있습니다.

Dell Technologies의 연결 소프트웨어는 고객 환경에서 시스템 및 이벤트 데이터를 전송하는 용도로만 사용됩니다. 텔레메트리는 Dell 백엔드로 안전하게 전송되어 Dell AIOps용 AI 알고리듬을 통해 분석됩니다.

37: TechDirect 포털에서 활성 지원 계약이 있는 연결된 Dell 인프라스트럭처 제품을 보고 관리할 수 있습니까?

아니요. TechDirect에서는 연결된 Dell 인프라스트럭처 제품을 보거나 관리할 수 없습니다. Dell Technologies의 연결 소프트웨어는 TechDirect와 통합되어 있지 않으므로, 연결된 Dell 시스템에 대한 알림 데이터 및 자동화된 지원 케이스는 포털의 대시보드에서 지원되거나 표시되지 않습니다.

하지만 온라인 지원 사이트와 MyService360 분석 대시보드에서 게이트웨이, 직접 연결 및 플러그인 옵션을 통해 연결된 Dell 시스템에 대한 자동화된 지원 케이스 세부 정보에 액세스하고 이를 관리할 수 있습니다.