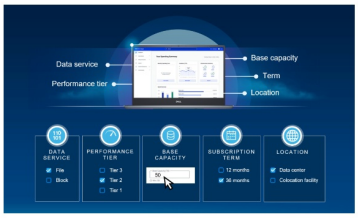

Remote Access Considerations for Dell Managed APEX Data Storage Services User Guide

August 2022
Rev. A02
Remote Access Considerations for Dell Managed APEX Data Storage Services Colocation and On-Premises Deployments

Contents

Remote Access Considerations for Dell Managed APEX Data Storage Services

Revision history

Table 1. Document revision history

Date	Document revision	Description of changes
August-22	A02	Updated the Farewells and port requirements section.
July-22	A01	Updated the document title. Updated Tables 4. 5. and 6 in the Firewalls and port requirements section.
May-22	A00	Initial release.

Remote Access Agreement

This Remote Access Considerations for Dell-Managed APEX Data Storage Services supplements the Service Offering
Description for APEX Data Storage Services which governs the dell offering.
Topics:

- Introduction
- Dell Management Stack
- Firewalls and port requirements

Introduction

Network connectivity is required between the front end hosted in Dell data centers and the Dell Management Stack (MS) at the site. A secure Connection Gateway is required for the successful implementation of APEX Data Storage Services. You are responsible for Internet services. Dell is responsible for the MS equipment and management at the site. Your company and Dell cooperate to maintain the operational status of the network connection between the parties.
The network design for remote connectivity requires a highly secure protocol adhered to by both Dell and your company. You must adhere to Dell's standard protocol configuration as advised during Service Enablement, and as updated by Dell as needed at Dell's absolute discretion.

Dell Management Stack

The MS is a standardized set of product element tools. These tools reside on each APEX Data Storage Service instance in a segregated Management Workload Domain used to provide the following MS functions:

- Support functions: Configuration management, remote support, troubleshooting, COTS–3rd party integration, and ticketing automation using the DELL Discovery Gateway
- Telemetry data collection:
  - Dell AIOps Gateway as the monitoring, event management, and alerting tool
  - Dell Secure Connection Gateway to gather telemetry data from the product elements
  - Discovery server to perform assets discovery
- Connectivity functions: Secure connectivity for transferring telemetry data between the APEX Data Storage Service instance at the site and the management platform using standard protocols with DELL Secure Connection Gateway
- Orchestration and control: Running automation tasks against Next Generation Cloud Services (NGCS) and

ServiceNow assets as defined in the DELL Automation Gateway

- APIs or element managers: API integrations between the product elements and the DELL AIOps Gateway and Secure Connection Gateway are set up to allow for direct configuration and policy management of the product elements
- Local intelligence: Error detection, auto incident creation, and event deduplication and consolidation to prevent “ticket storms”

Establishing a secure network

Establishing a secure network ensures that data is secured and that only authorized users and devices can use it. Establishing proper connectivity with Dell and other management systems is a critical first step to allow Dell to configure Management Zone and establish the services. The following describes exactly what must be provided to ensure that the service timeline is met.

Discovery server

The Discovery server is used to discover existing and ongoing provisioning resources. The data is made available to you so you can understand the provisioning resources you consume. Using the Software as a Service portal, you can request or perform other actions relating to the provisioning resources.

Dell AIOps Gateway

The services that leverage the Dell AIOps Gateway are:

- Discovery: Discover the resources on registered devices.
- Monitoring: Monitoring assesses the availability and performance of the managed resources. Monitoring is done by collecting, storing, and evaluating resource metrics.
  - Hardware failures
  - Server CPU utilization thresholds exceeded
  - Application failures
  - Configuration change
- Automation: Automation acts on resource faults, remediating issues in response to events, or performing routine maintenance tasks.
- Access controls: Access controls authorize user access to the platform and authenticate users.

Dell AIOps Gateway—Colocation and On-Premises deployments
The Dell AIOps Gateway is a comprehensive Software as a Service platform for IT operations management. The Gateway helps
IT teams control hybrid IT operations with a digital operations command center.
A Gateway is a virtual appliance that discovers and monitors devices such as VMs and hypervisor-based infrastructure, network elements, such as switches, routers, firewalls, and storage.
Dell AIOps Gateway—On-Premises deployments only
The following must be provided for the services to work:

- The Gateway must be able to reach out on the Internet and connect to the Software as a Service back-end system for registration and connectivity.
- The Gateway uses a secure TLS 1.2 connection to communicate and send data back to the Software as a Service platform.

This must be allowed on the network for the gateway to work.

- All required ports must be opened between the gateway and your environment for external connectivity. For more information, see the Firewall and Ports Requirements section.

Secure connection gateway

The services that leverage the Dell Secure Connection Gateway are as follows:

- Telemetry: By default, Secure Connection Gateway collects and sends device telemetry from all connected devices. The device telemetry is collected based on the predefined day and time. It also collects telemetry automatically from a device when a support case is created for an issue with the device.
- Monitoring: The Secure Connection Gateway monitors connected devices for any hardware issue and sends alerts back to
  Dell for support.
- Remote access: The Secure Connection Gateway has remote access capabilities. The Secure Connection Gateway allows the support team to connect securely to the end device for troubleshooting and remediation.
  ○ Remote access is also used to connect and initiate automation workflow to an automation-virtual machine (VM) in the MS.
  This automated process triggers when users send a request to the APEX Console.

Secure connection gateway—Colocation deployments
The Secure Connection Gateway is a highly secure connection between Dell and the APEX Data Storage Service instance at the site. Connectivity to the APEX Data Storage Service instance uses API calls on ports 443 and 8443. Dell configures the Secure
Connection Gateway between the APEX Data Storage Service instance and Dell for APEX Data Storage Service in a colocation.
Establishing a Secure Connection Gateway ensures that data is secure and that only authorized users and devices can use it.
Proper connectivity is critical to enable Dell to configure the Management Zone and establish the services.
Secure connection gateway—On-Premises deployments
The Secure Connection Gateway is a highly secure connection between Dell and your data center. Connectivity to your location uses API calls on ports 443 and 8443.
Establishing a Secure Connection Gateway ensures that data is secure and that only authorized users and devices can use it.
Proper connectivity is critical to enable Dell to configure the Management Zone and establish the Services.
The following must be provided for the services to work:

- The Gateway must be able to connect to the Dell backend system for registration and connectivity through the Internet.
- All required ports must be opened between the Gateway and the external environment for connectivity. For more information, see the Firewalls and port requirements section.

Security at a Dell

Security at a Dell—Colocation deployments
The MS deploys with the solution at the Dell Colocation Facility. Firewall rules are explicitly allowed on a required basis with traffic justification.
All-access to and from the Management Zone is controlled using firewall rules or access control lists (ACLs). The exact components at the Dell Colocation Facility depend on the information you provide. Your key inputs provide details about the low-level design including the communication ports used.

Only authorized team members can connect or view notifications from the system and all communications are bilaterally authenticated with RSA digital certificates.

Security at a Dell—On-Premises deployments

The MS deploys with the solution at your site. The firewall rules are explicitly allowed on a required basis and with traffic justification.

All-access to and from the Management Zone is controlled using firewall rules or ACLs. The exact components at your site depend on the information you provide. Your key inputs provide details about the low-level design including the communication ports used.

Only authorized team members can connect or view notifications from the system and all communications are bilaterally authenticated with RSA digital certificates.

Firewalls and port requirements

Dell security server ports

Table 2. Tenable

Purpose	From	To	Protocol/ Port	Traffic domain
Connect to SaaS Portal	Management Stack	cloud.tenable.com	TCP/ 443	Outbound

Table 2. Tenable (continued)

Purpose	From	To	Protocol/ Port	Traffic domain
Connect to SaaS Portal	Management Stack	*.nessus.org	TCP/ 443	Outbound

Table 3. EDR: Carbon Black Firewall Requirements for AWS Cloud

Purpose	From	To	Protocol/Port	Traffic domain
CB Device Services	Management Stack	dev-prod05.conferdeploy.net	TCP/443	Outbound
CB Content Management	Management Stack	content.carbonblack.io	TCP/443	Outbound
AV Definition Update Server	Management Stack	updates2.cdc.carbonblack.io	TCP/443	Outbound
Online Certificate Status Protocol (OCSP)	Management Stack	ocsp.godaddy.com	TCP/80	Outbound
Certificate Revocation List (CRL)	Management Stack	crl.godaddy.com	TCP/80	Outbound

The Endpoint Standard Sensor relies on the operating system for dynamic proxy detection.

Some third-party products such as McAfee EPO Gateway may attempt to validate the Carbon Black Cloud server certificate and terminate the connection due to a name mismatch between the certificate that is issued to the Carbon Black Cloud Login URL and the Service that the Endpoint Standard Sensor is connected to. In this event, the third party must be configured to not validate the domain certificate.

Although TCP requires bidirectional and full duplex communications, only outbound traffic to the above domains is

required from the sensor's perspective as the sensor initiates the TCP handshake. The stateful firewall performs network address translation (NAT) and routes traffic accordingly.
To determine whether the agent is "onsite" or "offsite," the sensor sends an Internet Control Message Protocol (ICMP) echo to see if the Domain Name Service (DNS) suffix address is reachable. In this case, you may observe outbound connections to your domain controllers from the Sensor Service (RepMgr).

Table 4. Anti-virus

Purpose	From	To	Protocol/ Port	Traffic domain
McAfee Management Services (MVision)	Management Stack	*.mvision.mcafee.com	TCP/ 80, 443	Outbound

NOTE: Port 80 is used for daily definition file updates (DAT/AMCORE).

Table 5. Dell discovery server

Purpose	From	To	Protocol/Port	Traffic domain
Connect to SaaS Portal	Management stack	dellsvcs.service-now.com	TCP/ 443	Outbound
	Management stack	install.service-now.com	TCP/ 443	Outbound
	Management stack	*http://ocsp.entrust.net/	TCP/ 443 TCP/80	Outbound

Table 6. Dell secure connection gateway

Purpose	From	To	Protocol/Port	Traffic domain
Connect to Dell Secure Remote Services (SRS) Backend	Management stack	esrs3-core.emc.com	TCP/ 443, 8443	Outbound
	Management stack	esrs3-coredr.emc.com	TCP/ 443, 8443	Outbound

Table 6. Dell secure connection gateway (continued)

Purpose	From	To	Protocol/Port	Traffic domain
	Management stack	esr3gduprd01-06.emc.com	TCP/ 443, 8443	Outbound
	Management stack	esr3ghoprd01-06.emc.com	TCP/ 443, 8443	Outbound
	Management stack	esr3gckprd01-12.emc.com	TCP/ 443, 8443	Outbound
	Management stack	esr3gscprd01-06.emc.com	TCP/ 443, 8443	Outbound
	Management stack	esr3gspprd01-06.emc.com	TCP/ 443, 8443	Outbound

Table 7. Dell AIOps Gateway

Purpose	From	To	Protocol/Port	Traffic dom ain
Connect to Dell AIOps Ga teway using the public IP address	Management stack	*.opsramp.com	TCP/443 TLS/443	Outbound
	Management stack	k8s.gcr.io	TCP/80 TCP/443	Outbound
	Management stack	us-docker.pkg.dev	TCP/80 TCP/443	Outbound
	Management stack	-.googleusercontent.com	TCP/80 TCP/443	Outbound
	Management stack	-.googleapis.com	TCP/443	Outbound
	Management stack	-.docker.io	TCP/443	Outbound
	Management stack	-.docker.com	TCP/443	Outbound

Table 8. General Port Requirements for all VMs

Purpose	From	To	Protocol/Port	Traffic domain
NTP	All Dell Management VMs	Customer NTP serv ers	UDP 123	Outbound
DNS	All Dell Management VMs	Customer NTP serv ers	TCP/UDP 53	Outbound
HTTP or HTTPS	All Dell Management VMs	HTTP or HTTPS sit e for support	TCP 80, 443	Outbound
SMTP	Dell File and Block Sto rage System	Customer SMTP Se rvices	TCP 25	Outbound

Table 9. Security manage services

Purpose	From	To	Protocol/Port	Traffic domain
Logs forwarded	CPMS Appliances and Splunk enterprise	Syslog	TCP/514	Internal/Inbound
Splunk Forwarder t o Splunk Deployme nt server	Windows/Linux Server s	Splunk Deployer	TCP/8089	Outbound/Inboun d
Splunk Forwarding agent to Heavy For warder	Windows/Linux Server s	Splunk Heavy Forw arder	TCP/9997	Outbound

Table 10. Azure CPMS Images Share

Purpose	From	To	Protocol/Port	Traffic domain
Azure CPMS Images Share	Management stack	cpmsimagesprod.file.core.windows.net	TCP 433	Inbound

Documents / Resources

	DELL Remote Access Considerations for Dell Managed APEX Data Storage Services [pdf] User Guide Remote Access Considerations for Dell Managed APEX Data Storage Services, Remote Access Considerations, Dell Managed APEX Data Storage Services