Dell Integrated System for Microsoft Azure Stack Hub Tech Book

Abstract

This document describes the Dell Integrated System for Microsoft Azure Stack Hub with Dell Technologies servers, networking, backup, and encryption, and Microsoft application-development tools.

Dell Technologies Solutions

May 2023
Rev. H17021.25

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2021 - 2023 Dell Inc. or its subsidiaries. All rights reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

Chapter 1: Executive summary **7**
Business challenge 7
Benefits of Dell Integrated System for Microsoft Azure Stack Hub 7
Document purpose 7
Overview 7
Caution 7
Change matrix 7
Audience 12
We value your feedback 12

Chapter 2: Solution Overview **13**
Solution architecture and key components 13
Overview 13
Microsoft azure stack hub 14
Dell Technologies hardware lifecycle host 14
Dell Integrated System for Microsoft Azure Stack Hub tactical 14
Dell PowerEdge R840 server 14
Dell PowerEdge R640 server 14
Configuration options 14
Standard components 14
Services 17
Order and deployment workflow 18
Azure App Service 18

Chapter 3: Prerequisites **19**
Environmental requirements 19
Data source: Legal notice 20
Power distribution unit (PDU) power-drop requirements 21
Azure connection, identity store, and billing-model decisions 22
Choosing connection options and identity store 22
Choosing the Disconnect from Azure option 22
Choosing the identity store 22
Features that are impaired or unavailable in disconnected mode 23
Required customer-provided security certificates 24
Mandatory certificates 25
Optional PaaS certificates 26
Certificate requirements and validation 27
Generating Azure Stack Hub certificate signing requests 27
Required Extension Host certificates 28
Certificate validation 28
Additional information 28
License requirements 28
Overview 28
Azure Stack Hub licensing 28

Azure Stack Hub endpoints and customer port requirements....29
Ports and protocols (inbound)....29
Firewall publishing....29

Chapter 4: Hardware Infrastructure....30
Hardware components....30
Overview....30
PowerEdge R840 server for dense and GPU scale units....31
PowerEdge R740xd server for hybrid scale units....32
PowerEdge R640 server for HLH and all-flash scale units (GPU support)....33
PowerSwitch N3248TE-ON management switch....35
PowerSwitch S5248F-ON ToR switch....35
Cisco Nexus 93180YC-FX switch....35
Cisco Nexus 9348GC-FXP switch....35
Switch dimensions....36
Dell Integrated System factory-rack dimensions....36
Rail kit information....37
Dense scale unit configuration....37
Customer provided rack and pdu....38
Supported PDU options....42
Hybrid scale-unit configuration....44
Customer-provided rack and PDU....45
All-flash scale-unit configuration....50
Supported PDU options....53
All-flash tactical configuration....55

Chapter 5: Networking and Cabling....57
Networking....57
Overview....57
Network transceivers....58
Scale unit node network connectivity....59
Border connectivity....60
Dense configuration networking....60
Server and switch port connections....60
HLH management network connectivity....60
Scale-unit node connectivity....61
Hybrid configuration networking....62
Server and switch port connections....62
HLH management network connectivity....62
Scale-unit node connectivity....64
All-flash configuration networking....64
Server and switch port connections....64
HLH management network connectivity....64
Scale-unit node connectivity....66
Azure Stack Hub switch cabling....66
Server and switch port description references....66
N3248TE-ON BMC port map....66
S5248F-ON ToR 1 port map....67
S5248F-ON ToR 2 port map....68

Border Gateway Protocol routing..... 71
Static routing..... 72
Transparent proxy..... 73
Firewall integration..... 74
Deployment..... 75
Services..... 75
Registering Azure Stack Hub..... 75

Chapter 6: Operations and Management Software..... 76
Microsoft azure stack hub software..... 76
Microsoft Azure Stack Hub..... 76
Accessing Azure Stack Hub..... 76
Privileged Endpoint..... 77
Hardware lifecycle host software..... 77
Microsoft Windows Server 2019 Datacenter edition..... 77
Dell Technologies Secure Connect Gateway (SCG)..... 78

Chapter 7: Security..... 79
Security overview..... 79
Least-privilege authority..... 79
Secrets rotation..... 79
Overview..... 79
HLH-related password changes..... 80

Chapter 8: Maintaining the Solution..... 81
Monitoring and alerting in Azure Stack Hub..... 81
Patch and update..... 81
Node expansion..... 82
Overview..... 82
Node expansion workflow..... 82
Hardware components for node expansion..... 83
Node expansion prerequisites..... 84
Networking modification..... 84
Deployment services..... 84

Chapter 9: Backup and Recovery..... 85
Backup and recovery overview..... 85
Backup requirements..... 85
Tenant data backups..... 85
In-scope data backups..... 85
Microsoft PaaS resource providers..... 86
Web application BCDR strategy..... 86
Third-party solutions..... 86
Custom images and BLOB collateral for the marketplace..... 86
HLH deployment collateral backup..... 87
SMB target folder structure..... 87
Recovery from a catastrophic failure..... 87

Chapter 10: Conclusion..... 88

Summary....88

Appendix A: License Retrieval....89
Retrieving Dell Technologies licenses....89
iDRAC license....89
Retrieving your iDRAC licenses....89

Appendix B: Dell Technologies Support and Consulting Offerings....90
Azure Stack Hub implementation requirements....90
Custom scope offering....90
Fixed price/fixed scope offering....90
Field replacement of parts....91
ProSupport Plus for Enterprise....91
Consulting service offerings....92
Additional resources....92
Tools for using Azure and Azure Stack Hub....92
Online documentation....93

1

Executive summary

Topics:

- Business challenge
- Document purpose
- We value your feedback

Business challenge

Adopting a hybrid-cloud strategy as a means to achieving digital transformation can be complicated. Often, IT and the organization they support have processes, procedures, personnel, and tools that are not aligned for optimal cloud brokerage and consumption.

The most common hurdles to overcome are:

- Complexity of disaggregate applications and tools
- Cloud competency compared to Legacy IT
- Lack of confidence that anytime, anywhere, always-on availability is achievable
- Cost of acquisition is unaffordable

Enterprise IT organizations are expected to deliver a consistent user experience. Most public and private cloud implementations are not reflective of one another, which makes implementing all phases of the life cycle (acquisition, deployment, operation, and maintenance) an inefficient process.

Benefits of Dell Integrated System for Microsoft Azure Stack Hub

Dell Integrated System for Microsoft Azure Stack Hub ("Dell Integrated System") is engineered with Dell Technologies servers, networking, backup, encryption, and Microsoft application-development tools. Dell Technologies manages the component life cycle of the entire Dell Integrated System to ensure that all phases are repeatable and predictable. This robust, complete solution simplifies and delivers better results for IT and digital transformation to our customers.

Document purpose

Overview

This tech book describes the main components of the Dell Integrated System.

NOTE: All references to release dates refer to Dell Technologies releases, unless otherwise indicated.

Caution

The recommendations and guidelines in this guide are based on industry best practices, Microsoft Azure Stack Hub architecture requirements, and Dell Technologies lab testing. If you do not follow the recommendations and guidelines, the functionality and management of the solution might not work as designed or expected. Problem resolution might be limited, delayed, or not viable.

Change matrix

The following table lists the major changes for this document revision.

Table 1. Revisions

Date	During release	Revision	Description
May 2023	2303	H17021.25	Updated the All-flash scale-unit configuration section.
February 2023	2212	H17021.24	Removed support for the following: • OpenManage Enterprise • Open Manage Network Manager
July 2022	2207	H17021.23	• Added Secure Connect Gateway related information. • Removed all references to SAE. • Product name rebranding.
February 2022	2112	H17021.22	Updated the Dell Technologies four-node mini-transport rack for a hybrid unit figure
June 2021	2105	H17021.21	Corrections to tables 2, 3, and 4 regarding the capacity and performance options for dense, hybrid, and all-flash configurations
March 2021	2102	H17021.20	Updated Networking S3048-ON with PowerSwitch N3248-TE-ON in tables, text, and diagrams Updating product name from Networking to PowerSwitch for S5248-ON throughout document Update node expansion content and workflow
December 2020	2011	H17021.19	Corrected details for border connectivity diagram Replaced network topology diagram Removed some content and linked directly to Microsoft source instead Move SU node network connectivity and border connectivity to new sections
November 2020	2010	H17021.18	Added information about NVIDIA T4 GPU Moved switch cabling tables to new section
September 2020	2008	H17021.17	Updated S5048-ON switches to S5248F-ON switches in tables, text, and diagrams

Table 1. Revisions (continued)

Date	During release	Revision	Description
			Updated port mapping in tables and diagrams Added detail and diagram for Isilon storage option
August 2020	2005	H17021.16	Added content about GPU, Micron drives, and Isilon storage option
May 2020	2004	H17021.15	Changed Dell EMC product name from Cloud for Microsoft Azure Stack Hub to Integrated System for Microsoft Azure Stack Hub throughout document.
March 2020	2002	H17021.14	Changed Microsoft product name from Azure Stack to Azure Stack Hub solution throughout document Changed company name from Dell EMC to Dell Technologies throughout document
January 2020	1911	H17021.13	Updated network connectivity figures to correct legends for All-Flash, Hybrid, and Dense configurations
October 2019	1908	H17021.12	Update configuration option tables 2, 3, and 4 due to CPU upgrade
September 2019	1908	H17021.11	Minor updates throughout document and to some tables and figures Changed OpenManage Essentials to OpenManage Enterprise throughout Added references to Windows Server 2019
June 2019	1904	H17021.10	Renamed VxRack AS to Microsoft hybrid cloud integrated system or Azure Stack integrated system, as applicable Removed references to S4048-ON in hybrid configurations Renamed product configurations to dense, hybrid, all flash, and tactical Azure Stack
April 2019	1903	H17021.9	Updates including PowerEdge R840-based configuration and server information:

Table 1. Revisions (continued)

Date	During release	Revision	Description
			Added PowerEdge R840 server info to <Solution architecture and key components> Added new Table 2: Capacity and performance option for PowerEdge R840-based configuration to <Configuration options> Edited SSD capacity column in Table 4: Capacity and performance options for R640 all-flash configurations Added new Table 6: R840-based configuration environmental requirements to <Environmental requirements> Added R840 server info to Table 9: Power-drop requirements in <PDU power-drop requirements> Added R840 server to Table 19: Hardware components in <Hardware components> Added R840 server info and new Figure 5 in <Hardware components> Added <Dense scale-unit configuration> section with new figures in <Hardware components> Added <Dense configuration> section in <Networking>
March 2019	1902	H17021.8	Corrections to SSD capacity calculations in Table 3: Capacity and performance options for R740xd balanced configurations Minor updates including: Renamed configuration in Table 2: Capacity and performance options for R740xd balanced configurations Renamed configurations in Table 3: Capacity and performance options for R740xd balanced configurations Added new Figure 27: Dell EMC Tactical R640 Azure Stack (rear view)

Table 1. Revisions (continued)

Date	During release	Revision	Description
February 2019	1901	H17021.7	Addition of <Dell EMC Tactical Microsoft Azure Stack> content Minor changes to the following: Added weight in kg in Tables 5 and 6 in <Environmental requirements> Updated Figure 26 in <HLH management network connectivity> Correct typo in Figures 43 and 44 in <Azure Stack implementation requirements>
November 2018	1810	H17021.6	Changes to the following sections: Updated node expansion content and figures Added Cisco switch content Updated 16-node content
October 2018	1809	H17021.5	Addition of VxRack AS factory rack, server, and switch dimensions to <Hardware components>
September 2018	1808	H17021.4	Addition of <Node expansion> content Addition of <Required Extension Host certificates> content Changes to the following sections: • Added note regarding automated preview P&U to <Patch and update> • Updated Table 27: Deployment services • Updated content in <ProSupport Plus for Enterprise> • Added content in <Appendix B: Dell EMC Support and Consulting Offerings>
August 2018	1806	H17021.3	Addition of <Rail kit information> content Addition of <Appendix A: License Retrieval> content Changes to the following sections:

Table 1. Revisions (continued)

Date	During release	Revision	Description
			• Deleted **Size** column in Table 1 • Corrected the memory amount for the **High** configuration in Table 3 • Updated Figure 20 and Figure 21 to remove 2U Filler • Added note regarding passwords in <HLH-related password changes>
July 2018	1805	H17021.2	Corrections to data in: Table 6: All-flash configuration environmental requirements Table 7: Power-drop requirements
June 2018	1805	H17021.1	Addition of all-flash configuration content Changes to the following: Chapter 3: Prerequisites Chapter 4: Hardware Infrastructure Chapter 6: Security Chapter 8: Backup and Recovery
April 2018	1803	H17021	Original publication

Audience

This guide is intended for IT administrators, storage administrators, virtualization administrators, system administrators, IT managers, and personnel who evaluate, acquire, manage, maintain, or operate Microsoft environments.

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on the solution and the solution documentation. Contact Dell Technologies Solutions team with your comments.

Author: Chris Mahon, John Nguyen

Contributor: Robb Cuccia, Chris Mahon, Jyoti Tripathi

2

Solution Overview

Topics:

- Solution architecture and key components
- Configuration options
- Order and deployment workflow
- Azure App Service

Solution architecture and key components

Overview

The Dell Integrated System for Microsoft Azure Stack Hub is a fully engineered hybrid-cloud platform that is built on a Microsoft hybrid-cloud-integrated architecture. This architecture consists of common modular building blocks that scale linearly from 4 to 16 nodes in a scale unit. Dell Integrated System provides a simple, cost-effective solution that delivers multiple performance and capacity options to match any use case. The solution supports a wide variety of cloud-native applications and workloads.

Dell Integrated System is based on Microsoft Azure Stack Hub software and built with Intel Xeon Gold and Platinum processors. Dell Integrated System enables customers to start small and grow, scaling capacity and performance with minimal disruption. Scaling in predictable units ensures a “pay-as-you-grow” approach for future growth.

The following figure shows the solution architecture.

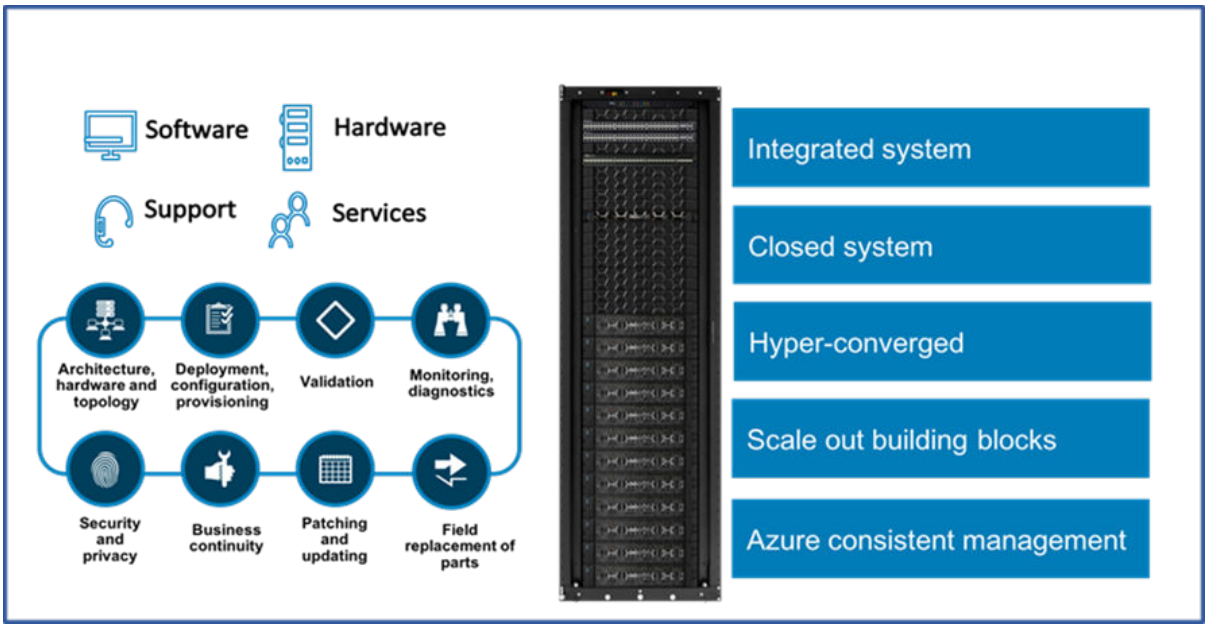

Figure 1. Dell Integrated System for Microsoft Azure Stack Hub architecture

Scale unit

Dell Integrated System is built around a scale unit, which is comprised of 4, 8, 12, or 16 identical nodes. As a hyperconverged platform, each node includes both compute and storage resources. Within the scale unit, the solution provides flexibility at a component level to optimize processor, memory, storage capacity, and caching ratios.

Microsoft azure stack hub

Microsoft Azure Stack Hub is an extension of Azure, bringing cloud computing to on-premises environments. You can build applications across hybrid-cloud environments, balancing flexibility and control. You can build applications using a consistent set of Azure services. You can speed up cloud-application development by building on application components from the Azure Marketplace, including open-source tools and technologies.

Dell Technologies hardware lifecycle host

The Dell Technologies hardware life cycle host (HLH) is designed to enable monitoring and updates for Dell Integrated System. The HLH is a Dell PowerEdge R640 management server. The HLH contains Dell Technologies management software and tools to enable server and network monitoring, and “call-home” capability. HLH also provides patch and update capability for the components that Dell Technologies provides.

Dell Integrated System for Microsoft Azure Stack Hub tactical

Dell Integrated System for Microsoft Azure Stack Hub tactical is a ruggedized and field-deployable product for Microsoft Azure Stack Hub. The product core components (servers, switches, and so on) are contained in pods protected by transit cases. The product core components are identical to our currently shipping all-flash data center Dell Integrated System offering.

A pod is a 4U rack container that has smaller dimensions than a regular 4U rack. There is one management pod and two scale unit pods. The management pod includes the hardware life cycle host (HLH), 25 GbE Top-of-Rack (ToR) switches, and a baseboard management switch.

Each scale unit pod holds two PowerEdge R640 scale unit servers. One PowerEdge R640 server occupies a 2U rack space in the pod. You can add additional PowerEdge R640 servers up to the full node limits of a Dell Integrated System all-flash scale unit node.

Dell PowerEdge R840 server

Dell PowerEdge R840 is a four-socket, 2U rack server that is designed to run complex workloads using highly scalable memory, I/O capacity, and network options. The PowerEdge R840 provides configurability to create an optimal configuration that balances solid-state drive (SSD) and hard-disk capacity.

As of the Dell Technologies 2011 release, several GPU options, NVIDIA V100, NVIDIA T4, and AMD Mi25, are available for some of the PowerEdge R840 and PowerEdge R640 configurations. A GPU provides higher throughput and parallel processing, which allows the system to process hundreds of transactions simultaneously.

PowerEdge R840 configurations are not expandable beyond the purchased configuration.

Dell PowerEdge R640 server

Dell PowerEdge R640 is a high-performance software-defined storage server. It is a two-socket, 1U rack server that is designed to run complex workloads by using highly scalable memory, I/O capacity, and network or GPU options. PowerEdge R640 provides an optimal server for use as an all-flash scale unit.

Configuration options

Standard components

The following table lists the scale units that are available. Each scale unit is associated with a server and configuration option.

Table 2. Scale units

Server	Configuration	Minimum nodes	Maximum nodes
Dell PowerEdge R740xd	Hybrid	4	16

Table 2. Scale units (continued)

Server	Configuration	Minimum nodes	Maximum nodes
Dell PowerEdge R640	All flash	4	16
Dell PowerEdge T-R640	Tactical all flash	4	16
Dell PowerEdge R840	Dense	4	16

The following tables list the capacity and performance options that each scale unit supports.

Table 3. Capacity and performance option for dense configuration

Configuration	Processor	Memory	SSD capacity
48-core	2 x Platinum 8260 24 cores, 2.4 GHz	1,532 GB	24 x 3.84 TB (92.16 TB) 2 x 32 GB NVIDIA V100s or 16 GB AMD Mi25 or 16 GB NVIDIA T4
96-core	4 x Platinum 8260 24 cores, 2.4 GHz	1,532 GB	24 x 3.84 TB (92.16 TB)

Table 4. Capacity and performance options for hybrid configurations

Configuration	Processor	Memory	Cache	Data storage
24-core	Gold 4214 12 cores, 2.2 GHz	384 GB	6 x 960/800 GB SSD = approx. 5.7 TB SAS	10 x 4 TB (40 TB) SAS
			6 x 1.92 TB (11.5 TB) SAS	10 x 8 TB (80 TB) SAS
				10 x 10 TB (100 TB) SAS (end of life)
				10 x 12 TB (120 TB) SAS
		576 GB	6 x 960/800 GB SSD = approx. 5.7 TB SAS	10 x 4 TB (40 TB) SAS
			6 x 1.92 TB (11.5 TB) SAS	10 x 8 TB (80 TB) SAS
				10 x 10 TB (100 TB) SAS (end of life)
				10 x 12 TB (120 TB) SAS
36-core	Gold 5220 18 cores, 2.2 GHz	384 GB	6 x 960/800 GB SSD = approx. 5.7 TB SAS	10 x 4 TB (40 TB) SAS
			6 x 1.92 TB (11.5 TB) SAS	10 x 8 TB (80 TB) SAS
				10 x 12 TB (120 TB) SAS
		576 GB	6 x 960/800 GB	10 x 4 TB (40 TB) SAS

Table 4. Capacity and performance options for hybrid configurations (continued)

Configuration	Processor	Memory	Cache	Data storage
			SSD = approx. 5.7 TB SAS	
			6 x 1.92 TB (11.5 TB) SAS	10 x 8 TB (80 TB) SAS
				10 x 12 TB (120 TB) SAS
		768 GB	6 x 960/800 GB SSD = approx. 5.7 TB SAS	10 x 4 TB (40 TB) SAS
			6 x 1.92 TB (11.5 TB) SAS	10 x 8 TB (80 TB) SAS
				10 x 12 TB (120 TB) SAS
40-core	Gold 6248 20 Cores, 2.5 GHz	576 GB	6 x 960/800 GB SSD = approx. 5.7 TB SAS	10 x 4 TB (40 TB) SAS
			6 x 1.92 TB (11.5 TB) SAS	10 x 8 TB (80 TB) SAS
				10 x 12 TB (120 TB) SAS
		768 GB	6 x 960/800 GB SSD = approx. 5.7 TB SAS	10 x 4 TB (40 TB) SAS
			6 x 1.92 TB (11.5 TB) SAS	10 x 8 TB (80 TB) SAS
				10 x 12 TB (120 TB) SAS
40-core	Gold 6248R 20 Cores, 2.5 GHz	768 GB	6 x 960/800 GB SSD = approx. 5.7 TB SAS	10 x 4 TB (40 TB) SAS
			6 x 1.92 TB (11.5 TB) SAS	10 x 12 TB (120 TB) SAS
		1,536 GB	6 x 1.92 TB (11.5 TB) SAS	10 x 12 TB (120 TB) SAS
48-core	Platinum 8260 24 cores, 2.4 GHz	768 GB	6 x 960/800 GB SSD = approx. 5.7 TB SAS	10 x 4 TB (40 TB) SAS
			6 x 1.92 TB (11.5 TB) SAS	10 x 8 TB (80 TB) SAS
				10 x 12 TB (120 TB) SAS
		1,536 GB	6 x 960/800 GB SSD = approx. 5.7 TB SAS	10 x 4 TB (40 TB) SAS
			6 x 1.92 TB (11.5 TB) SAS	10 x 8 TB (80 TB) SAS
				10 x 12 TB (120 TB) SAS

Table 5. Capacity and performance options for all-flash configurations

Configuration	Processor	Memory	SSD capacity
24-core	Gold 4214 12 cores, 2.2 GHz	384 GB	10 x 1.92 TB (19.2 TB)
		576 GB	
		768 GB	
36-core	Gold 5220 18 cores, 2.2 GHz	576 GB	10 x 1.92 TB (19.2 TB)
			10 x 3.84 TB (38.40 TB)
		768 GB	10 x 1.92 TB (19.2 TB)
			10 x 3.84 TB (38.40 TB)
40-core	Gold 6248 20 Cores, 2.5 GHz	768 GB	10 x 1.92 TB (19.2 TB)
			10 x 3.84 TB (38.40 TB)
48-core	Platinum 8260 24 cores, 2.4 GHz	768 GB	10 x 3.84 TB (38.40 TB)

NOTE: The capacity and performance options must be homogenous. You cannot mix and match within an scale unit.

Each scale unit also includes the required HLH server and network switches as listed in the following table.

Table 6. Capacity and performance options for all-flash configurations

Switch	Quantity	Hybrid configuration	All-flash configuration
Management server (HLH)	1	Dell PowerEdge R640	Dell PowerEdge R640
Top-of-rack (ToR)	2	Dell PowerSwitch S5248F-ON	Dell PowerSwitch S5248F-ON Cisco Nexus 93180YC-FX **NOTE:** Cisco switch is only available in a customer-provided rack For details, see <Rail kit information>.
Management (Mgt)	1	Dell PowerSwitch N3248TE-ON	Dell PowerSwitch N3248TE-ON Cisco Nexus 9348GC-FXP **NOTE:** Cisco switch is only available with the customer-rack option For details, see <Rail kit information>.

Services

The solution includes the following services offerings:

- Dell Technologies Support Services
- Dell Technologies Deployment Services
- Dell Technologies or Partner Professional Consulting Services (optional)

Order and deployment workflow

The following figure shows the workflow for customer delivery and deployment of Dell Integrated System.

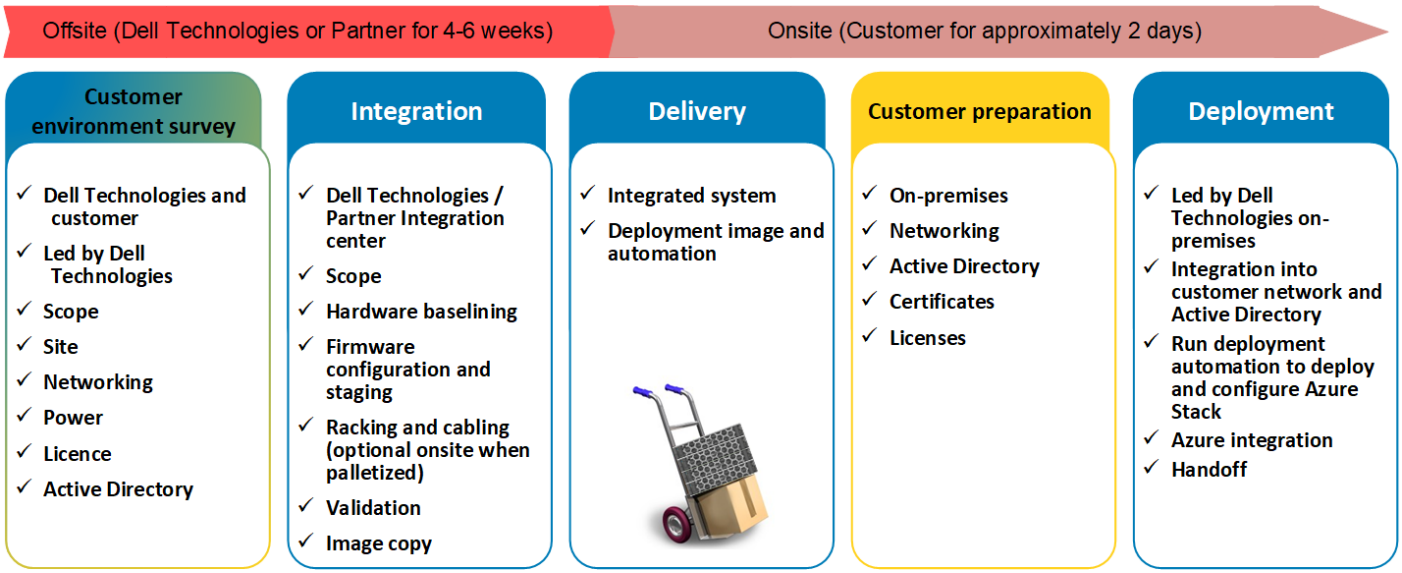

Figure 2. Delivery and deployment workflow

Azure App Service

The solution is designed to run infrastructure and platform services consistent with what is available from Azure.

For information about Azure App Services, see App Service overview on the Microsoft website.

3

Prerequisites

Topics:

- Environmental requirements
- Power distribution unit (PDU) power-drop requirements
- Azure connection, identity store, and billing-model decisions
- Choosing connection options and identity store
- Features that are impaired or unavailable in disconnected mode
- Required customer-provided security certificates
- Mandatory certificates
- Optional PaaS certificates
- Certificate requirements and validation
- License requirements
- Azure Stack Hub endpoints and customer port requirements

Environmental requirements

The following tables list the environmental requirements for a solution with different configurations of:

- 14 GB SUs
- 200-volt AC input voltage
- 35°C maximum ambient temperature

Table 7. GPU environmental requirements

Object	4-node		8-node	
Watts	BTU/hr	Watts	BTU/hr	
NVIDIA V100s GPU				
Input power	7,159	24,400	13,391	45,600
Input current (amps) at 200 V_{IN}	35.8		68.0	
Weight	880 lbs (399 kg)		1,204 lbs (546 kg)	
AMD Mi25 GPU				
Input power	7,159	24,400	13,391	45,600
Input current (amps) at 200 V_{IN}	35.8		68.0	
Weight	880 lbs (399 kg)		1,204 lbs (546 kg)	
NVIDIA T4 GPU				
Input power	4009	13,679	6,621	22,591
Input current (amps) at 200 V_{IN}	18.4		30.0	
Weight	880 lbs (399 kg)		1,204 lbs (546 kg)	

Table 8. Dense configuration environmental requirements

Object	4-node		8-node		12-node		16-node	
Watts	**BTU/hr**	**Watts**	**BTU/hr**	**Watts**	**BTU/hr**	**Watts**	**BTU/hr**	
Input power	5,630	19,200	10,411	35,500	15,161	51,700	19,941	68,000
Input current (amps) at 200 V_{IN}	28.4		52.4		76.4		100.4	
Weight	880 lbs (399 kg)		1204 lbs (546 kg)		1,593 lbs (693 kg)		2301 lbs (1,044 kg) 2 racks	

Table 9. Hybrid configuration environmental requirements

Object		4-node		8-node		12-node		16-node	
Watts	**BTU/hr**	**Watts**	**BTU/hr**	**Watts**	**BTU/hr**	**Watts**	**BTU/hr**		
Input power	Min config.	3,395	11,577	5,979	20,388	8,563	29,200	11,147	38,011
	Mid config.	3,691	12,586	6,571	22,407	9,451	32,228	12,331	42,049
	Max config.	3,927	13391	7,043	24,017	10,159	34,642	13,275	45,268
Input current (amps)	Min config.	17.2		30.3		43.4		56.5	
	Mid config.	18.7		33.3		47.8		62.4	
	Max config.	19.9		35.6		51.4		67.1	
Weight		790 lbs (358 kg)		1,082 lbs (491 kg)		1,374 lbs (623 kg)		1,666 lbs (756 kg)	

Table 10. All-flash configuration environmental requirements

Object		4-node		8-node		12-node		16-node	
Watts	**BTU/hr**	**Watts**	**BTU/hr**	**Watts**	**BTU/hr**	**Watts**	**BTU/hr**		
Input power	Min config.	2,620	8,800	4,360	14,600	6,090	20,400	7,830	26,200
	Max config.	3,410	11,500	5,930	20,000	8,460	28,500	10,980	37,100
Input current (amps)	Min config.	13.1		21.8		30.5		39.7	
	Max config.	17.05		29.7		42.3		54.9	
Weight		703 lbs (319 kg)		899 lbs (408 kg)		1,096 lbs (497 kg)		1,292 lbs (586 kg)	

Data source: Legal notice

Results shown in Table 6 through Table 9 are from Dell Technologies lab measurements and the Dell Power Calculator. The Dell Power Calculator is subject to change without notice and is provided “as is” without warrant of any kind, express or implied. Dell Technologies does not make any representations regarding the use, validity, accuracy, or reliability of the tool or the results of the use of the tool. The entire risk arising out of the use of this tool remains solely with the customer. In no event shall Dell Technologies be liable for any direct, consequential, incidental, special, punitive, or other damages, even if Dell Technologies is negligent or has been advised of the possibility of such damages arising from use of the tool or the information that is provided herein.

Output values that are obtained from this tool are intended solely for customer facilities planning purposes and are approximate and conservative. Actual results may vary.

Power distribution unit (PDU) power-drop requirements

The following table lists the power drops required for each number of SUs.

Table 11. Power-drop requirements

Number of SU nodes	Required number of power drops		
Single phase	Three-phase Delta	Three-phase Wye	
Dense			
4	2	1	1
8	3	1	1
12	4	2	1
16	5	3	2
Hybrid			
4	2	2	2
8	4	2	2
12	6	2	2
16	8	4	2
All flash			
4	2	2	2
8	4	2	2
12	4-6 *	2	2
16	6-8 *	2-4 *	2

* You need a higher number of power drops if you order these nodes with Intel Xeon 6248R processors.

The integrated system enables you to use different PDU connector types to best integrate into your data center, as listed in the following table.

Table 12. PDU and connector options

Location	Single phase	Three-phase Delta	Three-phase Wye
North America, Japan	L630P L7-30P Russellstoll 3750DP	Hubbell Pro CS8365L Russellstoll 9P54U2T/1100	Hubbell C530P6S ABL Sursum S52S0A Flying Leads
International	IEC60309-332P6W	Russellstoll 9P54U2T/1100	Hubbell C530P6S ABL Sursum S52S30A Flying Leads
Australia	Clipsal 56PA332		

Azure connection, identity store, and billing-model decisions

WARNING: Warning: Choosing Azure Active Directory (AAD) or Active Directory Federation Services (ADFS) is a one-time decision that you must make during deployment. You cannot change this decision later without redeploying the entire system.

For the latest information, see Azure Stack Hub integrated systems connection models on the Microsoft website.

Choosing connection options and identity store

Choosing the Disconnect from Azure option

If you choose the **Disconnect from Azure** option, you can deploy and use Microsoft Azure Stack Hub without a connection to the Internet. Choose this option if you:

- Have security or other restrictions that require you to deploy Azure Stack Hub in an environment that is not connected to the Internet.
- Want to block data (including usage data) from being sent to Azure.
- Want to use Azure Stack Hub purely as a private-cloud solution that is deployed to your corporate intranet, and are not interested in hybrid scenarios.

Table 13. Options that are based on physical connection

Options	Physically disconnected	Physically connected
Billing	Must be capacity Enterprise agreements (EA) only	Capacity or consumption EA or Cloud Solution Provider (CSP)
Identity store	Must be ADFS	AAD or ADFS
Marketplace syndication	Not applicable	Supported “Bring your own” licensing of syndicated images
Registration	Not applicable	Automated
Patch and update	Required, requires removable media and a separate connected device	Automated

NOTE: A physically disconnected environment is sometimes known as a “submarine scenario.”

With a disconnected deployment, you are limited to an ADFS identity store and a capacity-based billing model.

A disconnected deployment means that you will not have connectivity to Azure during deployment, or you do not want to use AAD as your identity store. However, you can later connect your Azure Stack Hub instance to Azure for hybrid scenarios for tenant virtual machines (VMs).

If you want to have connectivity to Azure after deployment, regardless of what you want to use as your identity store, choose the **Connect to Azure** deployment option.

Choosing the identity store

With a connected deployment, you can choose between AAD and ADFS for your identity store. A disconnected deployment can only use ADFS.

Your identity store choice has no bearing on tenant VMs, the identity store, and accounts that they use, whether they can join an Active Directory Domain, and so on.

For example, you can deploy IaaS tenant VMs on top of Azure Stack Hub and join them to a corporate Active Directory domain, from which you can use accounts. You are not required to use the AAD identity store for those accounts.

AAD identity store

When you use AAD for your identity store, you need two AAD accounts. These accounts can be the same account or different accounts. While using the same account might be simpler and useful if you have a limited number of Azure accounts, your business needs might require two accounts—global and billing:

- **Global admin account (only required for connected deployments)**—This Azure account is used to create applications and service principals for Azure Stack Hub infrastructure services in AAD. This account must have directory admin privileges to the directory under which the Azure Stack Hub system is deployed. It becomes the Global Admin for the AAD tenant. It is used:
- To provision and delegate applications and service principals for all Azure Stack Hub services that need to interact with AAD and Graph API.
- As the Service Administrator account, which owns the default provider subscription (which you can later change). You can log in to the Azure Stack Hub admin portal with this account. Use it to create offers and plans, set quotas, and perform other administrative functions in Azure Stack Hub.
- **Billing account (required for both connected and disconnected deployments)**—This Azure account is used to establish the billing relationship between your Azure Stack Hub system and the Azure commerce back end. This account is billed for Azure Stack Hub fees. It is also used for marketplace syndication and other hybrid scenarios.

ADFS identity store

Choose this option if you want to:

- Use your own identity store, such as Active Directory, for your Service Administrator accounts.
- Use your corporate Active Directory to manage your Service Administrator accounts.

Features that are impaired or unavailable in disconnected mode

Microsoft Azure Stack Hub is designed to work best when connected to Azure. The following table lists some features and functionality that are either impaired or unavailable in the disconnected mode.

Table 14. Impacted features and functionality

Feature/functionality	Impact in disconnected mode
VM deployment with DSC extension to configure VM post deployment	**Impaired**—DSC extension looks to the Internet for the latest WMF.
VM deployment with Docker Extension to run Docker commands	**Impaired**—Docker checks the Internet for the latest version and this check fails.
Documentation links in the Azure Stack Hub Portal	**Unavailable**—Links that use an Internet URL, such as Give Feedback, Help, Quickstart, and so on, do not work.
Alert remediation/mitigation that references an online remediation guide	**Unavailable**—Any alert remediation links that use an Internet URL do not work.
Marketplace syndication – The ability to select and add Gallery packages directly from the Azure Marketplace	**Impaired**—When you deploy Azure Stack Hub in a disconnected mode (without any Internet connectivity), you cannot download Marketplace items through the Azure Stack Hub Portal. However, use the Marketplace Syndication tool to download the Marketplace items to a computer that has Internet connectivity, and then transfer the items to your Dell Integrated System.
Using Azure Active Directory federation accounts to manage an Azure Stack Hub deployment	**Unavailable**—Requires connectivity to Azure. ADFS with a local Active Directory instance must be used instead.

Table 14. Impacted features and functionality (continued)

App Services	**Impaired**—WebApps might require Internet access for updated content.
Command Line Interface (CLI)	**Impaired**—The CLI has reduced functionality for authentication and provisioning of Service Principles.
Visual Studio – Cloud discovery	**Impaired**—Cloud Discovery either discovers different clouds or does not work at all.
Visual Studio – ADFS	**Impaired**—Only Visual Studio Enterprise supports ADFS.
Telemetry	**Unavailable**—Telemetry data for Azure Stack Hub and any third-party Gallery packages that depend on telemetry data are not available.
Certificates	**Unavailable**—Internet connectivity is required for Certificate Revocation List (CRL) and Online Certificate Status Protocol (OSCP) services in the context of HTTPS.
Key Vault	**Impaired**—A common scenario for Key Vault is to have an application read secrets at runtime, which requires a service principal in the directory. In AAD, non-administrator users are permitted, by default, to add service principals, but in Active Directory (using ADFS), they are not. This scenario affects the end-to-end experience because users must always go through a directory admin to add an application.

For the latest information, see Azure disconnected deployment planning decisions for Azure Stack Hub integrated systems on the Microsoft website.

Required customer-provided security certificates

Microsoft Azure Stack Hub has a public infrastructure network that contains the externally accessible or public IP addresses that are assigned to a small set of Azure Stack Hub services, with the remainder used by the tenant VMs. Provide certificates with the appropriate DNS names for these Azure Stack Hub public infrastructure endpoints.

There are some certificate restrictions in the current Azure Stack Hub version. The certificate requirements for deploying Azure Stack Hub are:

- Certificates must be issued from either an internal certificate authority or a public certificate authority. If a public certificate authority is used, it must be included in the base operating-system image as part of the Microsoft Trusted Root Authority Program. For the full list, see TechNet Microsoft Trusted Root Certificate Program: Participants.
- Your Azure Stack Hub infrastructure must have network access to the certificate authority Certificate Revocation List (CRL) location published in the certificate. This CRL must be an HTTP endpoint.
- When you rotate certificates, certificates must be either issued from the same internal certificate authority that is used to sign certificates that are provided at deployment or any public certificate authority from the CRL.
- The certificate can be a single wildcard certificate covering all name spaces in the Subject Alternative Name (SAN) field. Alternatively, you can use individual certificates using wildcards for endpoints, such as ACS and Key Vault, where they are required.
- The certificate signature algorithm cannot be SHA1; it must be stronger.
- The certificate format must be PFX, because both the public and private keys are required for an Azure Stack Hub installation.
- The certificate PFX files must have the values **Digital Signature** and **KeyEncipherment** in the **Key Usage** field.
- The certificate PFX files must have the values **Server Authentication (1.3.6.1.5.5.7.3.1)** and **Client Authentication (1.3.6.1.5.5.7.3.2)** in the **Enhanced Key Usage** field.
- The certificate **Issued to:** field must not be the same as its **Issued by:** field.
- The passwords to all certificate PFX files must be the same at the time of deployment.
- The password for the certificate PFX must be a complex password.
- The subject names and subject alternative names in the SAN extension (x509v3_config) must match. The **subject alternative names** field enables you to specify additional host names (websites, IP addresses, common names) that are to be protected by a single SSL certificate.

NOTE: The use of self-signed certificates is not supported. Instead, the presence of intermediary certificate authorities in a certificate chain-of-trust is supported.

Mandatory certificates

The following table describes the Microsoft Azure Stack Hub public endpoint PKI certificates that are required for both AAD and ADFS Azure Stack Hub deployments. Certificate requirements are grouped by area, namespaces used, and the certificates that are required for each namespace. The table also describes the folder in which your solution provider copies the different certificates per public endpoint.

Table 15. Azure Stack Hub PKI certificate requirements (14G)

Deployment folder	Required certificate subject and SAN	Scope (per region)	Subdomain namespace
Public Portal	portal.<region>.<fqdn>	Portals	<region>.<fqdn>
Admin Portal	adminportal.<region>.<fqdn>	Portals	<region>.<fqdn>
Azure Resource Manager Public	management.<region>.<fqdn>	Azure Resource Manager	<region>.<fqdn>
Azure Resource Manager Admin	adminmanagement.<region>.<fqdn>	Azure Resource Manager	<region>.<fqdn>
ACSBlob	*.blob.<region>.<fqdn> (Wildcard SSL Certificate)	Blob Storage	blob.<region>.<fqdn>
ACSTable	*.table.<region>.<fqdn> (Wildcard SSL Certificate)	Table Storage	table.<region>.<fqdn>
ACSQueue	*.queue.<region>.<fqdn> (Wildcard SSL Certificate)	Queue Storage	queue.<region>.<fqdn>
KeyVault	*.vault.<region>.<fqdn> (Wildcard SSL Certificate)	Key Vault	vault.<region>.<fqdn>
KeyVaultInternal	*.adminvault.<region>.<fqdn> (Wildcard SSL Certificate)	Internal Keyvault	adminvault.<region>.<fqdn>
Extension Host	*.hosting.<region>.<fqdn> (Wildcard SSL Certificates)	Extension Host	hosting.<region>.<fqdn>
	*.adminhosting.<region>.<fqdn> (Wildcard SSL Certificates)	Extension Host	adminhosting.<region>.<fqdn>

Use certificates with the appropriate DNS names for each Azure Stack Hub public infrastructure endpoint. Each endpoint DNS name is expressed in the following format: <prefix>.<region>.<fqdn>.

For your deployment, the [region] and [externalfqdn] values must match the region and external domain names that you choose for your Azure Stack Hub system. For example, if the region name is “Redmond” and the external domain name is “company.com”, the DNS names have the format *<prefix>*.redmond.company.com. Microsoft predesignates the *<prefix>* values to describe the endpoint that is secured by the certificate. Also, the *<prefix>* values of the external infrastructure endpoints depend on the Azure Stack Hub service that uses the specific endpoint.

NOTE: You can provide certificates as single wildcard certificates covering all name spaces in the Subject and SAN fields that are copied into all directories. You can also provide certificates as individual certificates for each endpoint copied into

the corresponding directory. Both options require that you use wildcard certificates for endpoints, such as ACS and Key Vault, where they are required.

For Azure Stack Hub environments on pre-1803 release versions, see the following table. If you deploy Azure Stack Hub using the AAD deployment mode, you only need to request the certificates listed.

Table 16. Azure Stack Hub PKI certificate requirements (13G)

Deployment folder	Required certificate subject and SAN	Scope (per region)	Subdomain namespace
Public Portal	portal.<region>.<fqdn>	Portals	<region>.<fqdn>
Admin Portal	adminportal.<region>.<fqdn>	Portals	<region>.<fqdn>
Azure Resource Manager Public	management.<region>.<fqdn>	Azure Resource Manager	<region>.<fqdn>
Azure Resource Manager Admin	adminmanagement.<region>.<fqdn>	Azure Resource Manager	<region>.<fqdn>
ACS	One multi-subdomain wildcard certificate with Subject Alternative names for: *.blob.<region>.<fqdn> *.queue.<region>.<fqdn> *.table.<region>.<fqdn>	Storage	blob.<region>.<fqdn> table.<region>.<fqdn> queue.<region>.<fqdn>
KeyVault	*.vault.<region>.<fqdn> (Wildcard SSL Certificate)	Key Vault	vault.<region>.<fqdn>
KeyVaultInternal	*.adminvault.<region>.<fqdn> (Wildcard SSL Certificate)	Internal Keyvault	adminvault.<region>.<fqdn>

NOTE: The ACS certificate requires three wildcard SANs on a single certificate. Not all Public Certificate Authorities support multiple wildcard SANs on a single certificate.

However, if you deploy Azure Stack Hub using the ADFS deployment mode, you must also request the certificates that are described in the following table.

Table 17. Azure Stack Hub PKI certificate requirements (13G) with ADFS deployment

Deployment folder	Required certificate subject and SAN	Scope (per region)	Subdomain namespace
ADFS	adfs.<region>.<fqdn> (SSL Certificate)	ADFS	<region>.<fqdn>
Graph	graph.<region>.<fqdn> (SSL Certificate)	Graph	<region>.<fqdn>

Optional PaaS certificates

Note All certificates that are listed in this section must have the same password.

If you plan to deploy the additional Azure Stack Hub PaaS services (SQL, MySQL, and App Service) after Azure Stack Hub has been deployed and configured, you must request additional certificates to cover the endpoints of the PaaS services.

NOTE: The certificates that you use for SQL, MySQL, and App Service resource providers must have the same root authority as those certificates used for the global Azure Stack Hub endpoints.

The following table describes the endpoints and certificates that are required for the SQL and MySQL adapters and for App Service. You do not need to copy these certificates to the Azure Stack Hub deployment folder. Instead, provide these certificates when you install the additional resource providers.

Table 18. Certificates and endpoints for additional PaaS services

Certificate	Scope (per region)	Required certificate subject and SANs	Subdomain namespace
SQL and MySQL	SQL, MySQL	*.dbadapter.<region>.<fqdn> (Wildcard SSL Certificate)	dbadapter.<region>.<fqdn>
Web Traffic Default SSL Cert	App Service	*.appservice.<region>.<fqdn> *.scm.appservice.<region>.<fqdn> *.sso.appservice.<region>.<fqdn> (Multi Domain Wildcard SSL Certificate)	appservice.<region>.<fqdn> scm.appservice.<region>.<fqdn>
API	App Service	api.appservice.<region>.<fqdn> (SSL Certificate)	appservice.<region>.<fqdn> scm.appservice.<region>.<fqdn>
FTP	App Service	ftp.appservice.<region>.<fqdn> (SSL Certificate)	appservice.<region>.<fqdn> scm.appservice.<region>.<fqdn>
SSO	App Service	sso.appservice.<region>.<fqdn> (SSL Certificate)	appservice.<region>.<fqdn> scm.appservice.<region>.<fqdn>

NOTE: Notes: Multi Domain Wildcard SSL Certificate—Requires one certificate with multiple wildcard SANs. Not all Public Certificate Authorities support multiple wildcard SANs on a single certificate.

NOTE: Note: SSL Certificate—An *.appservice.<region>.<fqdn> wildcard certificate cannot be used in place of the following certificates: (api.appservice.<region>.<fqdn>, ftp.appservice.<region>.<fqdn>, and sso.appservice.<region>.<fqdn>. Appservice explicitly requires the use of separate certificates for these endpoints.

For more information about the public key infrastructure (PKI) certificates that are required to deploy Azure Stack Hub and how to obtain them, see Azure Stack Hub public key infrastructure certificate requirements on the Microsoft website.

Certificate requirements and validation

Generating Azure Stack Hub certificate signing requests

The Microsoft Azure Stack Hub Readiness Checker tool is available from the PowerShell Gallery. The tool creates Certificate Signing Requests (CSRs) for an Azure Stack Hub deployment. Certificates should be requested, generated, and validated with enough time to test before deployment.

The Azure Stack Readiness Checker tool (AzsReadinessChecker) performs the following certificate requests:

- **Standard Certificate Requests**—Request according to Generate PKI Certificates for Azure Stack Deployment
- **Request Type**—Specifies whether the Certificate Signing Request is a single request or multiple requests
- **Platform-as-a-service (PaaS)**—Optionally request PaaS names for certificates, as specified in the Azure Stack Hub public key infrastructure certificate requirements > Optional PaaS certificates

Required Extension Host certificates

The implementation of Microsoft Extension Host requires two wildcard SSL certificates, one for the admin portal and one for the tenant portal. Customers who have deployed Azure Stack Hub systems must provide these two additional certificates.

For more information, see Azure Stack Hub public key infrastructure certificate requirements > Validate.

Certificate validation

You can use the Azure Stack Readiness Checker tool to validate that the generated PKI certificates are suitable for predeployment. When you validate certificates, schedule enough time to test and get certificates reissued if necessary.

NOTE: Treat the PKI certificate PFX file and password as sensitive information.

Additional information

For the latest certificate requirements and validation instructions, see the Microsoft Azure Stack Hub public key infrastructure certificate requirements.

License requirements

Overview

An Azure subscription including Active Directory must be available before deploying Microsoft Azure Stack Hub. Purchase this subscription from Dell Technologies, Microsoft, or other providers.

The solution includes the required Dell Technologies and Microsoft licenses:

- Azure Stack Hub with Microsoft Windows Server 2019 Datacenter Edition

Azure Stack Hub licensing

The solution is licensed through pay-as-you-use metering and consumption billing. Azure Stack Hub consumption includes both public and private cloud workloads. Microsoft aggregates the metering information for this usage at regular intervals. The only licensing options that can be used for Azure Stack Hub consumption billing are enterprise agreements (EAs) and the Cloud Solution Provider (CSP) program.

For more information, see Microsoft Azure Stack Hub Pricing.

NOTE: The customer or partner is responsible for licensing any third-party software that is used in an Azure Stack Hub tenant.

Enterprise agreements are ideal for organizations that already use an EA for other Microsoft software programs. An EA offers complete control of the Azure subscriptions running on the stack solution. Azure Stack Hub use is applied to the monetary commitment in the EA, and support for the Azure services is provided directly from Microsoft. An EA is also the only method to license Azure Stack Hub if you want to run it in a disconnected mode. This capacity model requires an annual subscription.

As an Azure CSP Direct and Indirect provider, Dell Technologies offers consumption-based licensing on Azure Stack Hub to enterprise organizations and channel partners. Through CSP, Dell Technologies provides sales, provisioning, billing, and support. Dell Technologies bills enterprise customers on a monthly basis, but the CSP agreement is non-contractual. Dell Technologies partners using the CSP Indirect program bill their end-customers in the format the customer selects for their Azure use, whether bundled with other services or pass-through.

For more information, see Microsoft Azure in Cloud Solution Provider.

Azure Stack Hub endpoints and customer port requirements

Ports and protocols (inbound)

Microsoft provides tables of the ports and protocols in use by Azure Stack Hub. For the latest information, see Publish Azure Stack Hub services in your datacenter on the Microsoft website.

Firewall publishing

For information, see Azure Stack Hub firewall integration on the Microsoft website.

4

Hardware Infrastructure

Topics:

- Hardware components
- Switch dimensions
- Dell Integrated System factory-rack dimensions
- Rail kit information
- Dense scale unit configuration
- Hybrid scale-unit configuration
- All-flash scale-unit configuration
- All-flash tactical configuration

Hardware components

Overview

The following table lists the minimum hardware components that are required to deploy this solution.

Table 19. Hardware components

Component	Quantity	Details
Dell PowerEdge R740xd or Dell PowerEdge R640 or Dell PowerEdge R840	4–16	Minimum of 4 scale unit servers
Dell PowerEdge R640 HLH server	1	Management server for HLH
Dell PowerSwitch S5248F-ON switch or Cisco Nexus 93180YC-FX **NOTE:** Cisco switch is only available with the customer-rack option For details, see Rail kit information .	2	Top of Rack (ToR) switches
Dell PowerSwitch N3248TE-ON switch or Cisco Nexus 9348GC-FXP **NOTE:** Cisco switch is only available with the customer-rack option For details, see Rail kit information .	1	Management switch

Dimensions of the Dell Integrated System factory rack, switch components, and PowerEdge R840, R640, and R740xd servers are also included.

The following sections provide details about the primary hardware components.

PowerEdge R840 server for dense and GPU scale units

The PowerEdge R840 server is a four-socket, 2U rack system for demanding environments. It provides a balance between storage, I/O, and application acceleration with configuration flexibility.

In Dell Integrated System, the PowerEdge R840 server, which is shown in the following figure, is configured with 24 SSDs and two M.2 solid-state boot drives. There is also a GPU option available.

Figure 3. Dell PowerEdge R840 server

R840 server dimensions

The following figure shows the physical dimensions of the R840 server.

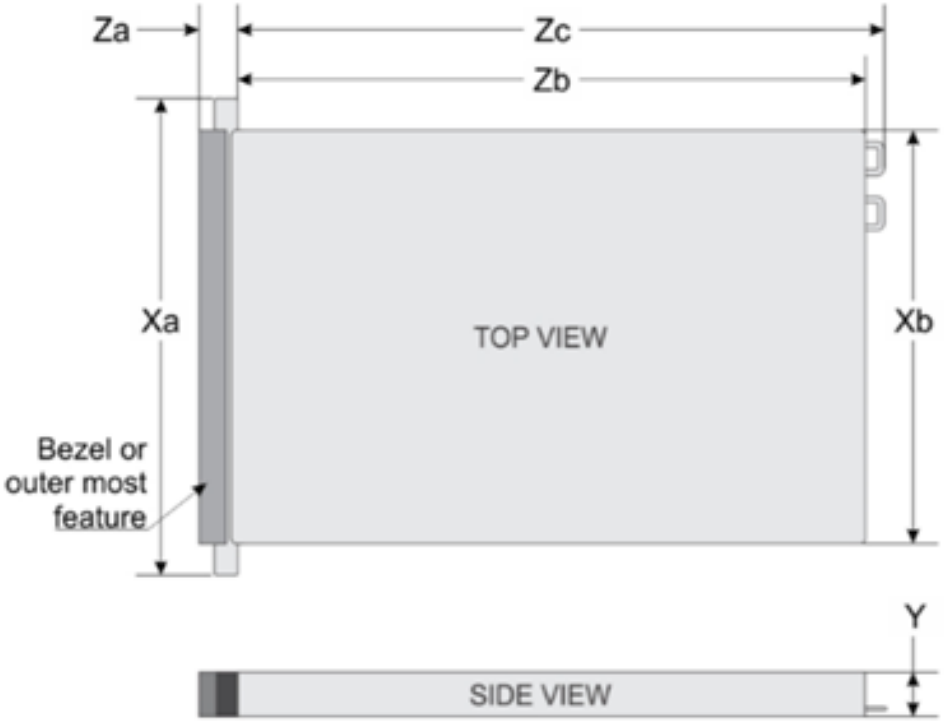

Figure 4. R840 server physical dimensions

The following table lists the measurements for the R840 server, which is shown in the previous figure.

Table 20. R840 server measurements legend

Measurement	Inches	Millimeters
Xa (Front Width)	18.97	482.00
Xb (Rear Width) – without brackets	17.08	434.00
Xb (Rear Width) – with brackets	17.48	444.00

Table 20. R840 server measurements legend (continued)

Y (Height)	3.41	86.80
Za (Forward Depth with Bezel)	1.41	37.84
Za (Forward Depth without Bezel)	0.94	23.90
Zb	31.96	812.00
Zc (Depth Behind Bezel) – with PSU handle	33.14	842.00
Zc (Depth Behind Bezel) – with chassis near wall handle	35.51	902.00

NOTE: Zb means the nominal rear wall external surface where the system board I/O connectors are located.

PowerEdge R740xd server for hybrid scale units

The PowerEdge R740xd server is a two-socket, 2U rack system for demanding environments. It provides a balance between storage, I/O, and application acceleration with configuration flexibility.

In Dell Integrated System, the PowerEdge R740xd server, which is shown in the following figure, is configured with 18 drives: 2 solid-state boot drives, 6 solid-state cache drives, and 10 HDDs for storage capacity.

Figure 5. Dell PowerEdge R740xd server

R740xd server dimensions

The following figure shows the physical dimensions of the R740xd server.

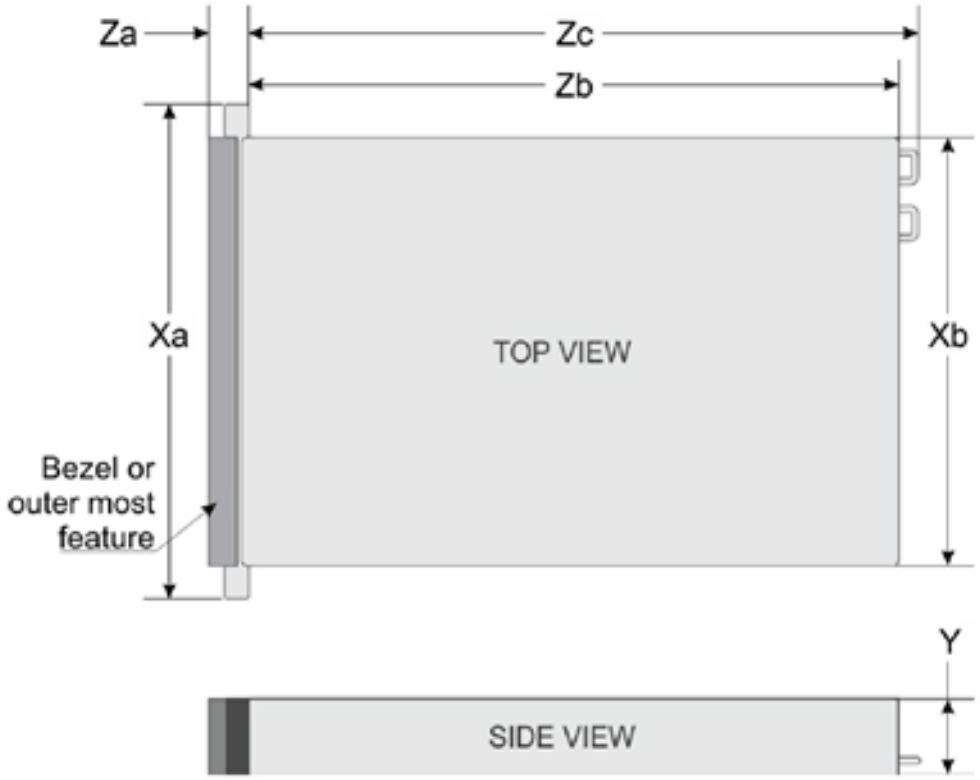

Figure 6. R740xd server physical dimensions

The following table lists the measurements for the R740xd server, which is shown in the previous figure.

Table 21. R740xd server measurements legend

Measurement	Inches	Millimeters
Xa (Front Width)	18.98	482.00
Xb (Rear Width)	17.09	434.00
Y (Height)	3.42 (2U)	86.80
Za (Forward Depth with Bezel)	1.41	35.84
Za (Forward Depth without Bezel)	0.87	22.00
Zb (Depth Behind Bezel)	26.72	678.00
Zc (Depth Behind Bezel)	28.17	715.50

PowerEdge R640 server for HLH and all-flash scale units (GPU support)

The PowerEdge R640 server, as shown in the following figure, is a scalable computing and storage rack in a 1U, two-socket platform with a balanced mix of performance, cost, and density for most data centers. When used as an all-flash SU, the server is configured with 12 drives: 2 solid-state boot drives and 10 solid-state flash drives. There is also an NVIDIA T4 GPU option.

Figure 7. Dell PowerEdge R640 server

R640 server dimensions

The following figure shows the physical dimensions of the R640 server.

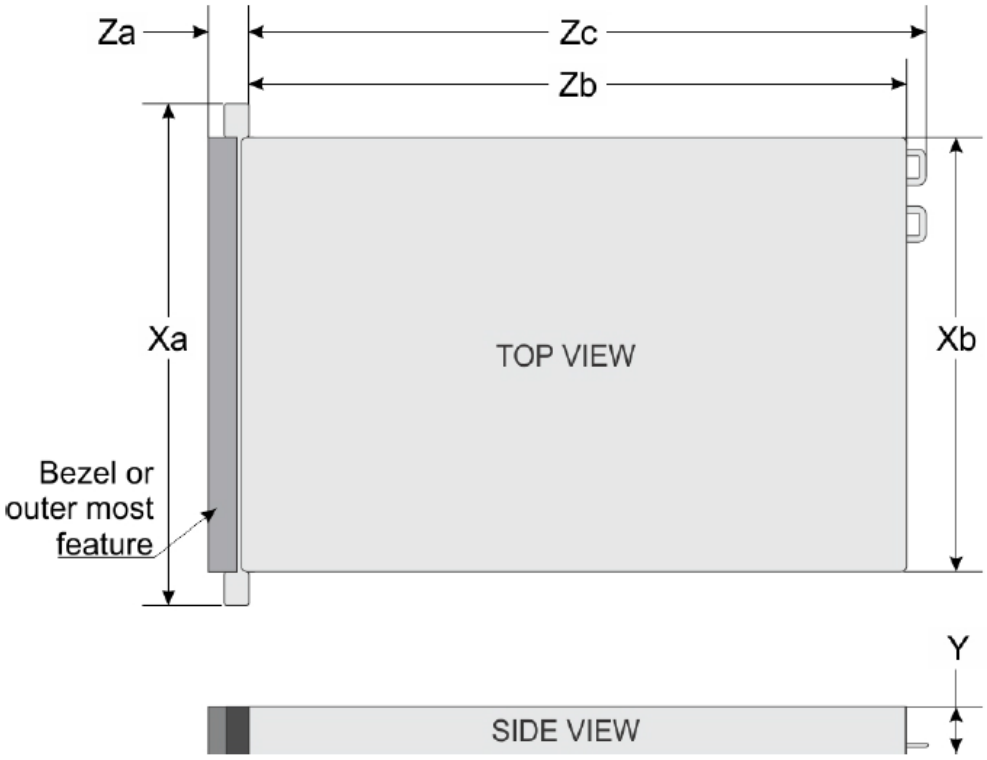

Figure 8. R640 server physical dimensions

The following table lists the measurements for the R640 server, which shown in the previous figure.

Table 22. R640 server measurements legend

Measurement	Inches	Millimeters
Xa (Front Width)	18.97	482.00
Xb (Rear Width)	17.08	434.00
Y (Height)	1.68 (1U)	42.80
Za (Forward Depth with Bezel)	1.41	35.84
Za (Forward Depth without Bezel)	0 .87	22.00
Zb (Depth Behind Bezel)	29.61	733.82
Zc (Depth Behind Bezel)	30.42	772.67

PowerSwitch N3248TE-ON management switch

The PowerSwitch N3248TE-ON is a 1/10/100 GbE management switch, as shown in the following figure, and is a high-performance switch that uses a non-blocking architecture to handle unexpected traffic loads. The switch is ideal for mid- to large-enterprise campus networks or retail deployments. The N3248TE-ON is a 1RU form-factor switch that features 48 x 1 GB RJ-45 with 802.3at (30 W) PoE ports, 4 x 10 GB SFP+ ports, and 2 x 100 GB QSFP28 ports.

Figure 9. Dell PowerSwitch N3248TE-ON switch

PowerSwitch S5248F-ON ToR switch

The PowerSwitch S5248F-ON is a 25/100 GbE fixed switch. The S5248F-ON is a Dell Technologies data-center networking solution. The switch provides high-density 25/100 GbE ports and a range of functionality to meet the growing demands of a data-center environment. The following figures shows the S5248F-ON, which is a 1-RU form-factor multilayer switch. It provides density with up to 48 ports of 25 GbE, 4 ports of 100 GbE, and 2 ports of 200 GbE.

Figure 10. Dell PowerSwitch S5248F-ON switch

Cisco Nexus 93180YC-FX switch

The Cisco Nexus 93180YC-FX switch can be used as a ToR switch.

This switch has 48 1/10/25 Gb/s Fiber ports and six 40/100 Gb/s QSFP28 ports.

NOTE: Cisco switch is only available with the customer-rack option. For details, see Rail kit information .

Figure 11. Cisco Nexus 93180YC-FX switch

Cisco Nexus 9348GC-FXP switch

The Cisco Nexus 9348GC-FXP switch can be used as a management switch.

This switch has 48 100M/1G BASE-T ports, four 10/25 Gb/s SFP28 ports, and two 40/100 Gb/s QSFP28 ports.

NOTE: Cisco switch is only available with the customer-rack option. For details, see Rail kit information .

Figure 12. Cisco Nexus 9348GC-FXP switch

Switch dimensions

The following table lists the physical dimensions of the switch components.

Table 23. Switch component physical dimensions

Component	Height	Width	Depth
N3248TE-ON Mgt switch	1.71 inches (1U) 43.50 mm	17.09 inches 434.00 mm	12.60 inches 320.00 mm
S5248F-ON ToR switch	1.72 inches (1U) 44.00 mm	17.1 inches 434.00 mm	18.1 inches 459.74 mm
Cisco Nexus 93180YC-FX ToR switch	1.72 inches (1U) 44.00 mm	17.3 inches 439.00 mm	22.5 inches 571.00 mm
Cisco Nexus 9348GC-FXP Mgt switch	1.72 inches (1U) 44.00 mm	17.3 inches 439.00 mm	19.7 inches 499.00 mm

NOTE: Cisco switch is only available with the customer-rack option. For details, see Rail kit information .

Dell Integrated System factory-rack dimensions

The following table lists the physical dimensions for a Dell Integrated System factory rack.

If you are using a different customer-supplied rack, we recommend that your rack has similar dimensions.

Table 24. Dell Integrated System factory-rack dimensions

Dimensions	Inches	Millimeters
Overall height	75.00 +/-0.060	1,905.00 +/-1.52
Overall width	24.00 +/-0.060	609.60 +/-1.52
Overall external depth	39.37 Front filler panel/device bezel to back surface of rear door	1,000.00 Front filler panel/device bezel to back surface of rear door
	41.50 Front door (optional) to back surface of rear door (based on configuration)	1,054.00 Front door (optional) to back surface of rear door (based on configuration)
Overall internal depth	36.94 Front outer surface of NEMA rail to inner surface of rear door	938.30 Front outer surface of NEMA rail to inner surface of rear door

Table 24. Dell Integrated System factory-rack dimensions (continued)

	38.68 Maximum from front cosmetic bezel to back surface of rear door	982.50 Maximum from front cosmetic bezel to back surface of rear door

Rail kit information

When a deployment uses customer-provided racks and PDU, mini racks are used to ship hardware from the Dell Technologies factory. The racks arrive at the customer location with servers and switches racked and stacked in them.

Each server (scale nodes and management server) and switch (ToRs and BMC) has rail kits that must be transferred to the customer-provided rack. The following table lists the rails for the servers and switches in the stack.

Table 25. Rails for stack servers and switches

Rail kit		Server associated with rail kit	Total rail kits shipped per node configuration	Rack type
Part number	**Name**			
100-564-836	Dell R730 sliding rail kit universal	R740xd (scale nodes)	4 kits for 4-node 8 kits for 8-node 12 kits for 12-node 16 kits for 16-node	40U rack and mini rack
100-564-837	Dell R630 sliding rail kit universal	R640 (HLH/ management server)	One kit for any-node configuration customer orders	40U rack and mini rack
100-564-837	Dell R630 sliding rail kit universal	R640 (all-flash scale nodes)	4 kits for 4-node 8 kits for 8-node 12 kits for 12-node 16 kits for 16-node	40U rack and mini rack
100-566-022	Dell Gen3.14 switch rail 22-inch offset	Dell switches	3 kits for any-node configuration customer orders	mini rack
100-566-039 or 100-400-187	Dell Gen3.14 switch rail 22-inch offset without pods or Dell Gen3 switch rail universal	Dell switches	3 kits for any-node configuration customer orders	40U rack and mini rack
106-590-021	MHC Cisco switch rail kit	Cisco switches	3 kits for any-node configuration customer orders	mini rack

Dense scale unit configuration

The PowerEdge R840 unit for the Dell Integrated System dense is available pre-racked in a Dell Technologies rack and PDU. It can also be ordered without the rack and PDU, and then integrated into a customer-provided dedicated rack and PDU.

NOTE: If you use a customer-provided rack and PDU, the customer must ensure that they have the required power and space for serviceability. For information, see Environmental requirements.

Customer provided rack and pdu

If the customer-provided rack and PDU option is selected, Dell Technologies configures the servers in its factory. It then ships the components in a mini-transport rack that is designed for convenient transport and availability of the components. The following figure shows a four-node Dell Integrated System—dense in a mini rack.

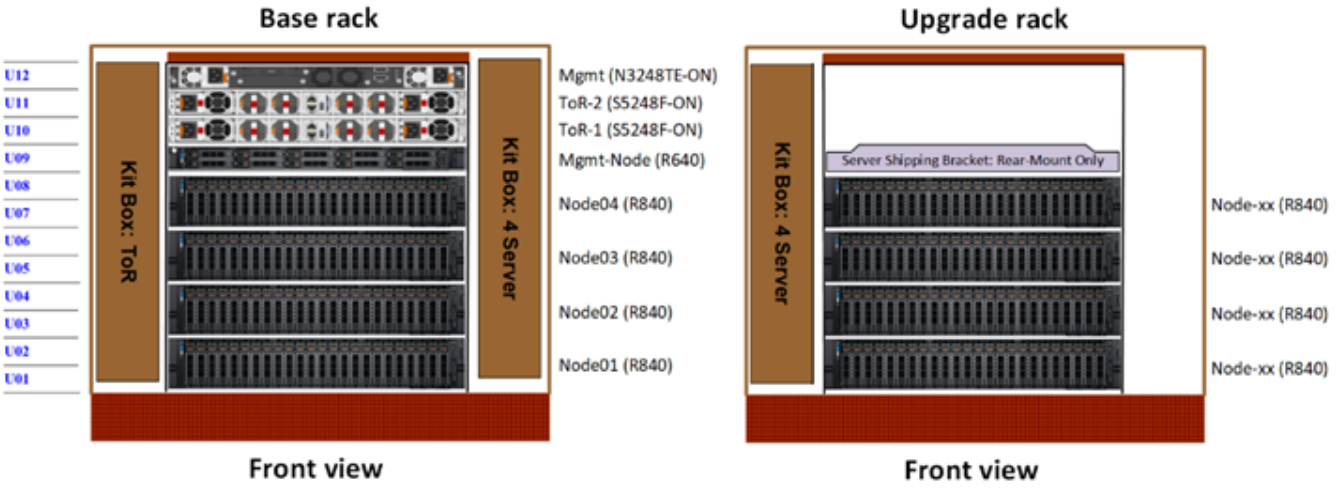

Figure 13. Dell Technologies four-node mini-transport rack for a dense uni

Dell Technologies service installs the components into the customer-provided rack before completing the Azure deployment.

The following table lists the number of mini racks that are shipped based on the number of SUs that are ordered.

Table 26. Configuration mini-rack requirements

Azure Stack Hub integrated system configuration	Required mini-racks
4 nodes	1
8 nodes	2
12 nodes	3
16 nodes	4

The following figures show switch and server placement for a minimum 4-node configuration up to 16-node configuration. The solution comes pre-racked, stacked, and cabled. It is ready for a Dell Technologies Engineer to configure into your data center and to complete the deployment as an IaaS platform.

Additional Dell Technologies consulting services are available to help you tailor Dell Integrated System for Microsoft Azure Stack Hub.

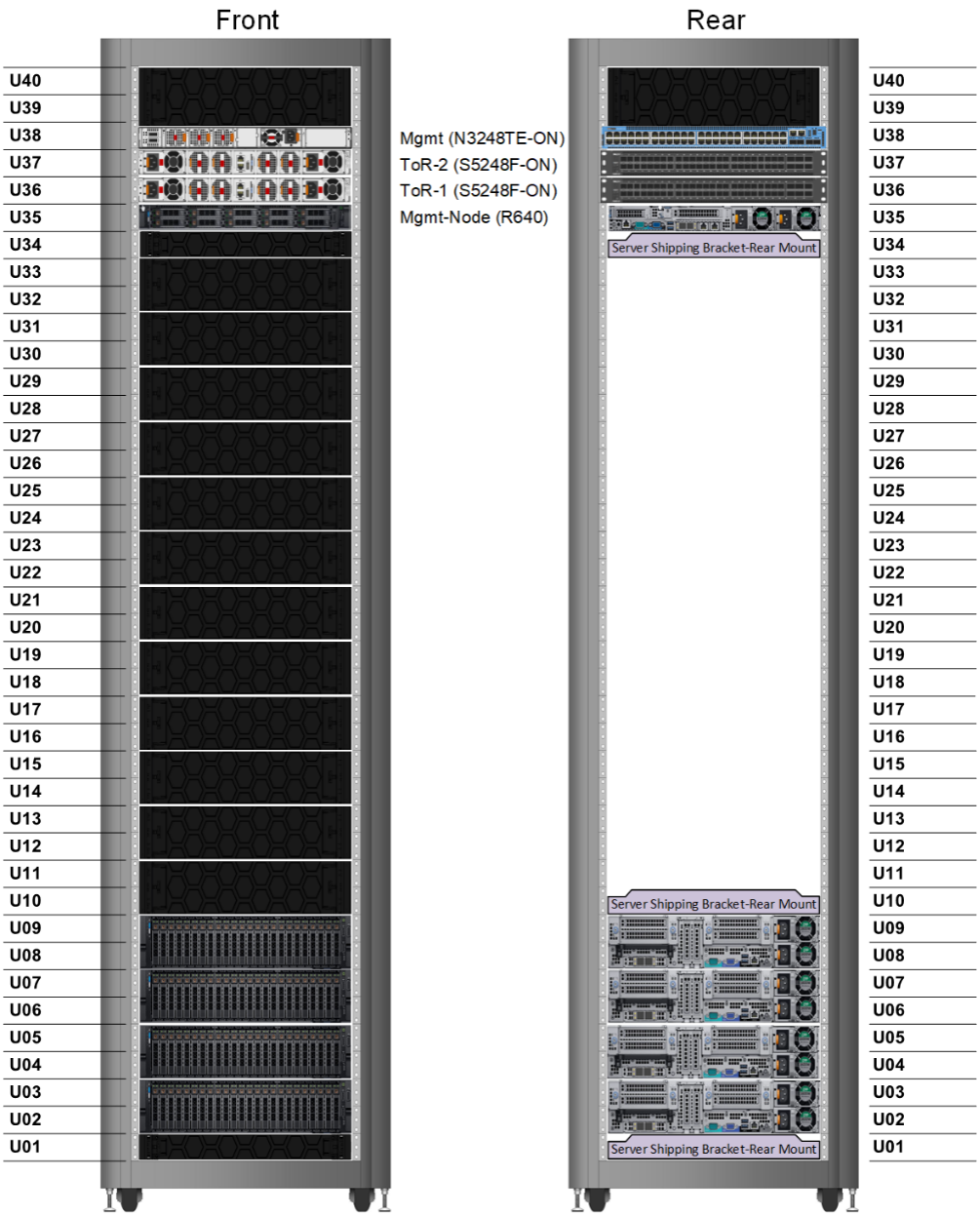

Figure 14. Minimum dense configuration elevation: 4-node SU

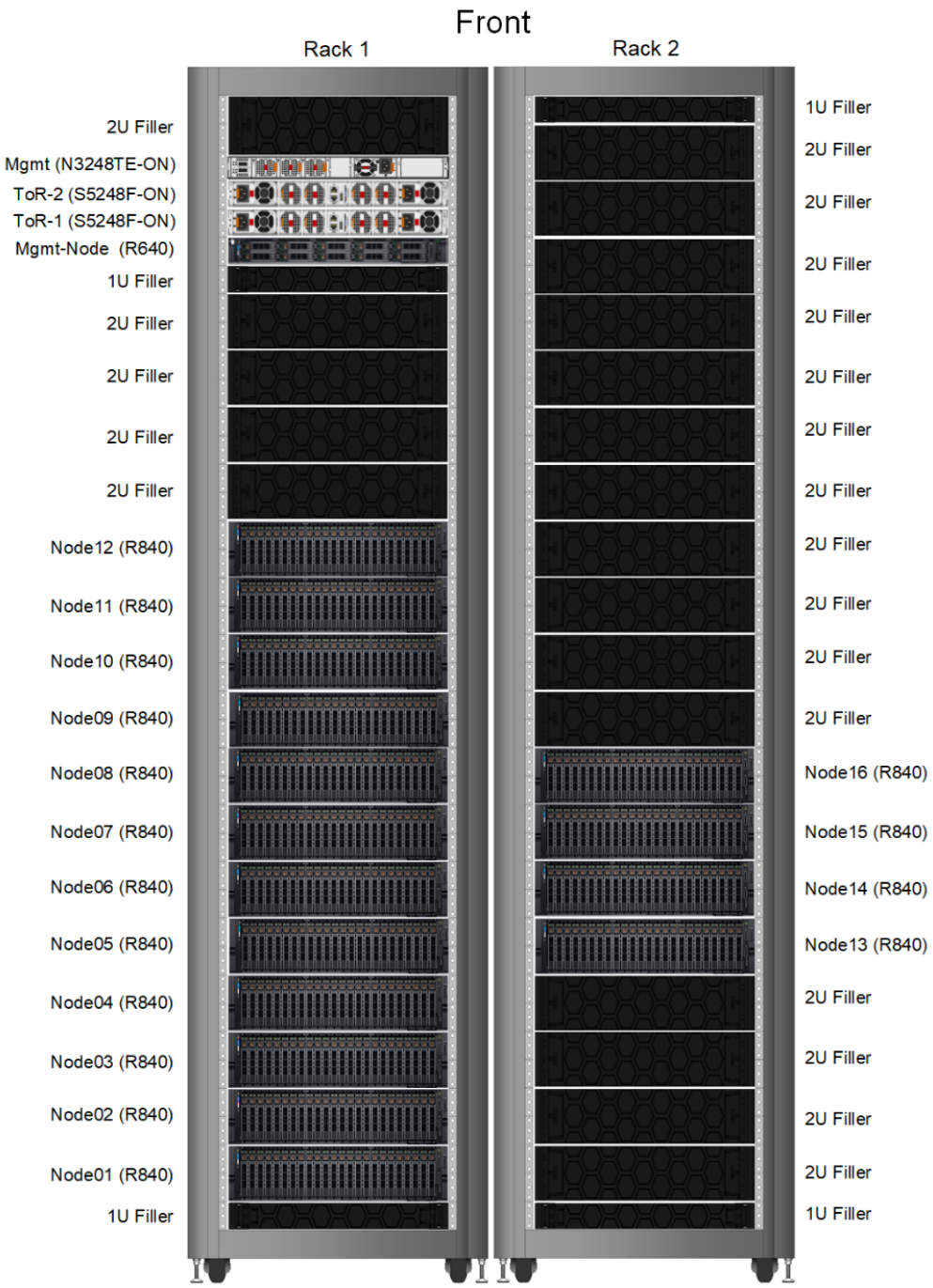

Figure 15. Maximum dense configuration elevation: 16-node SU (front view)

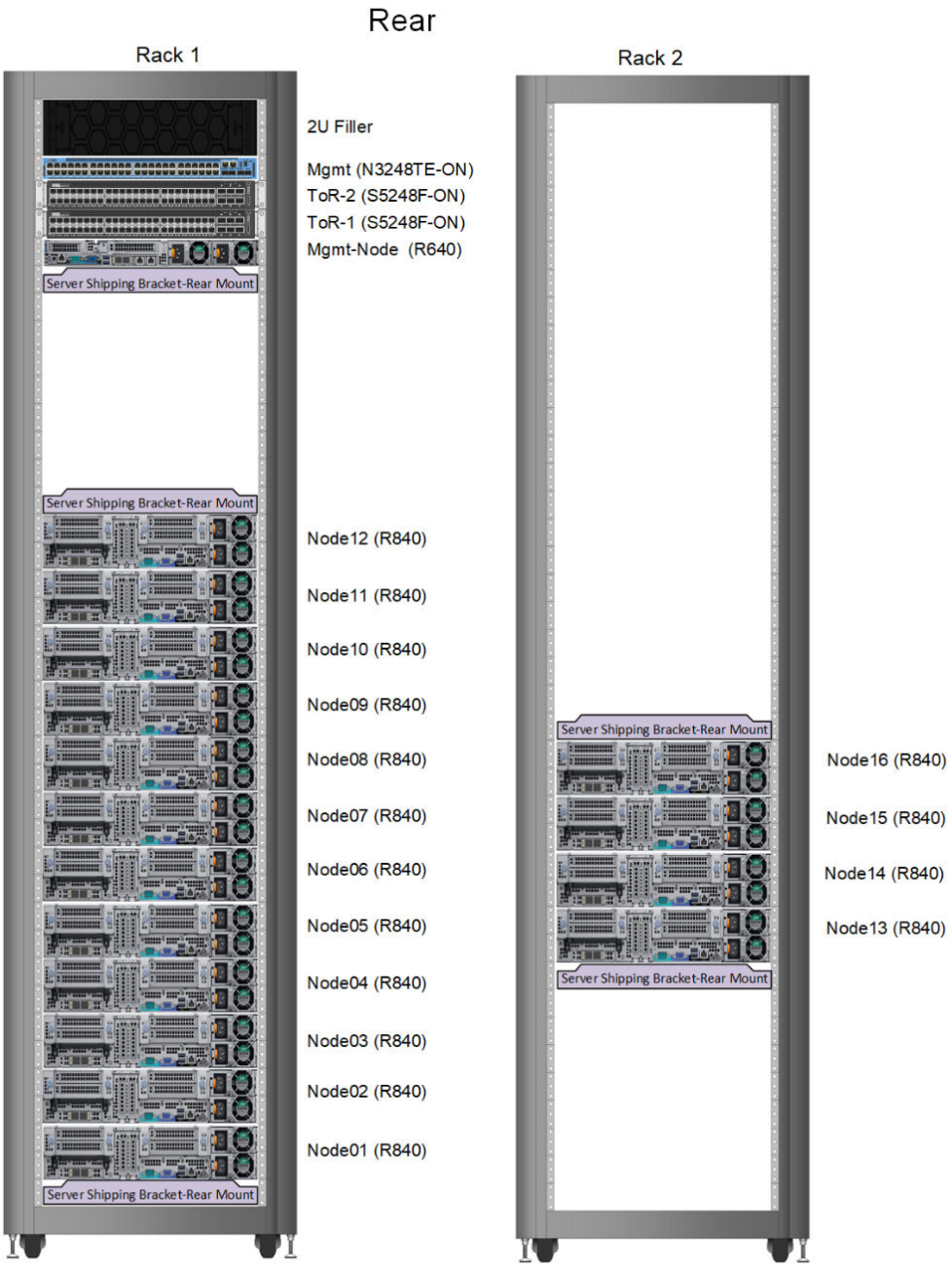

Figure 16. Maximum dense configuration elevation: 16-node SU (rear view)

Supported PDU options

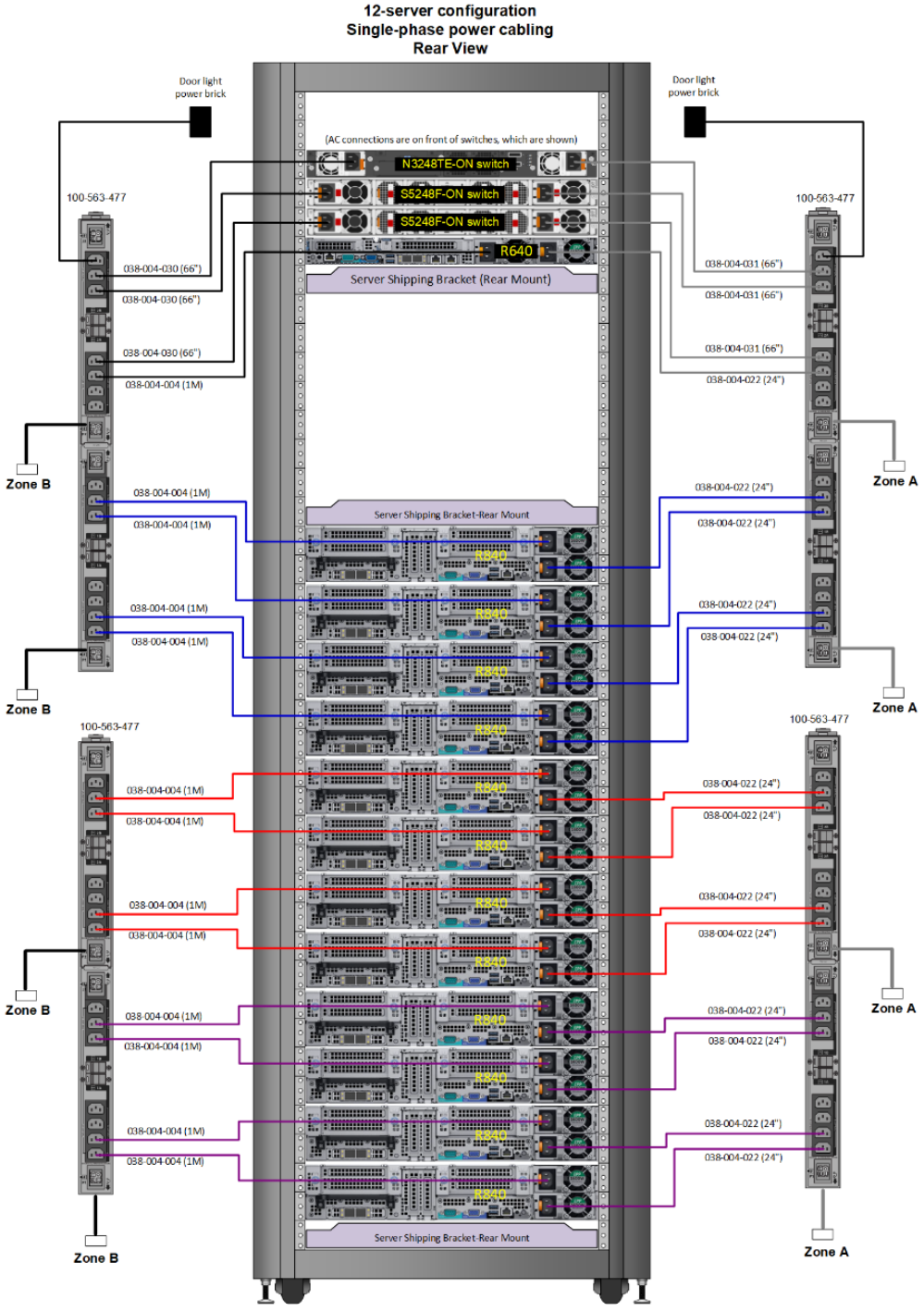

Figure 17. Dense configuration: Single-phase PDU

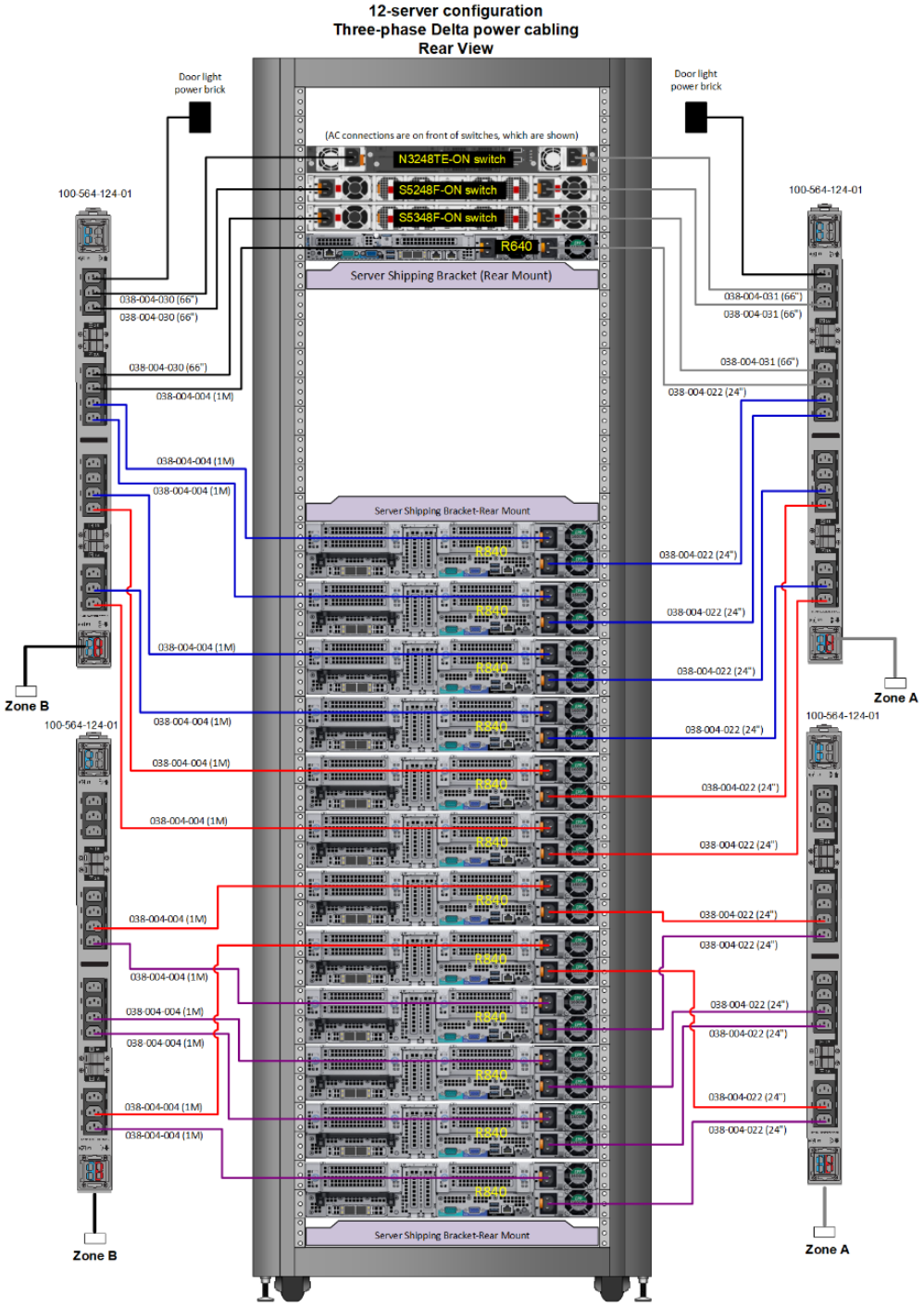

Figure 18. Dense configuration: Three-phase Delta PDU

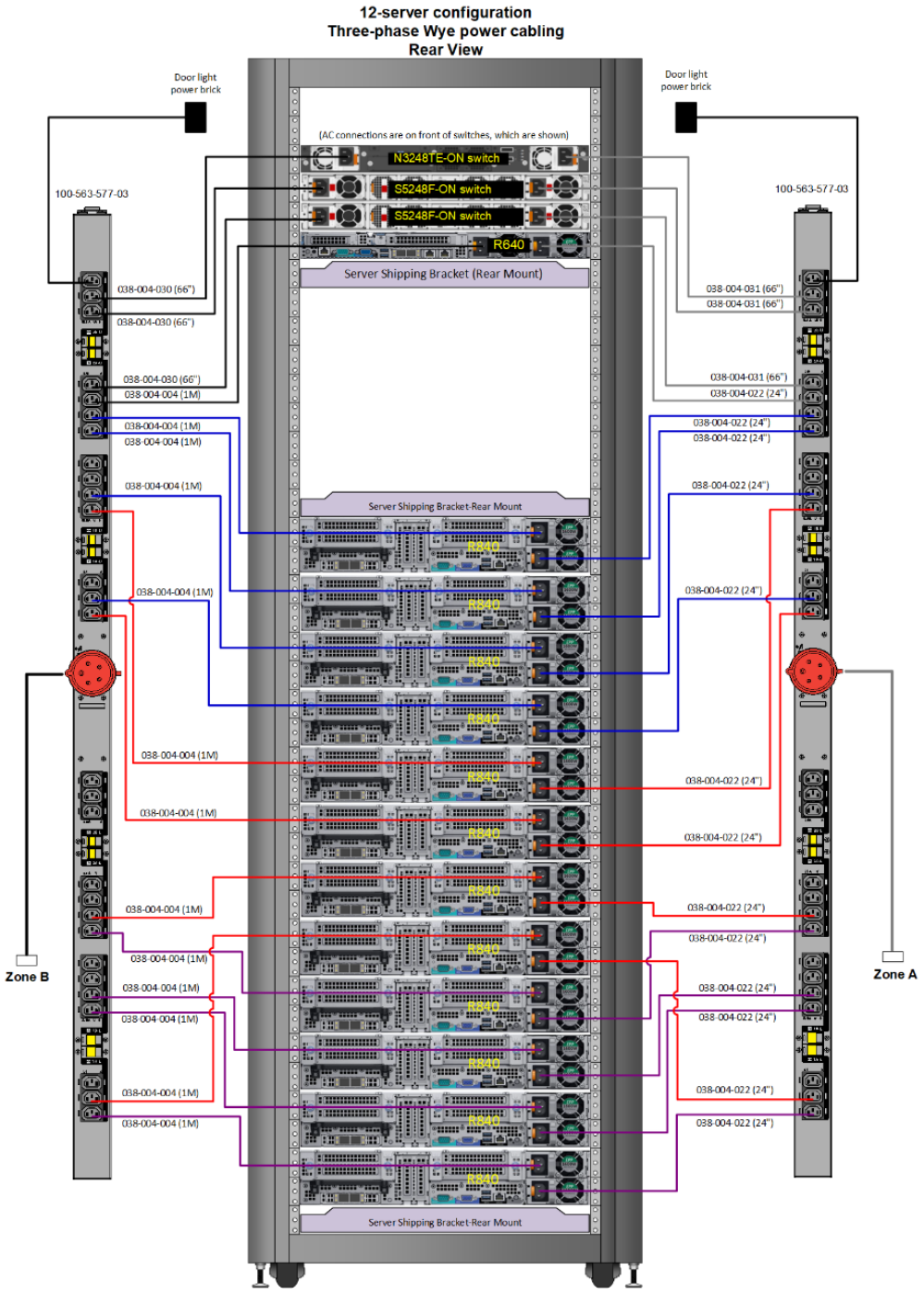

Figure 19. Dense configuration: Three-phase Wye PDU

Hybrid scale-unit configuration

Dell Integrated System hybrid is available pre-racked in a Dell Technologies rack and PDU. Optionally, you can order the Dell Integrated System hybrid without the rack and PDU, and integrate it into a customer-provided dedicated rack and PDU.

NOTE: If you use a customer-provided rack and PDU, the customer must ensure that they have the required power and space for serviceability. For information, see Environmental requirements.

Customer-provided rack and PDU

If the customer-provided rack and PDU option is selected, Dell Technologies configures the servers in its factory. It then ships the components in a mini-transport rack that is designed for convenient transport and availability of the components. The following figure shows a four-node Dell Integrated System—hybrid in a mini rack.

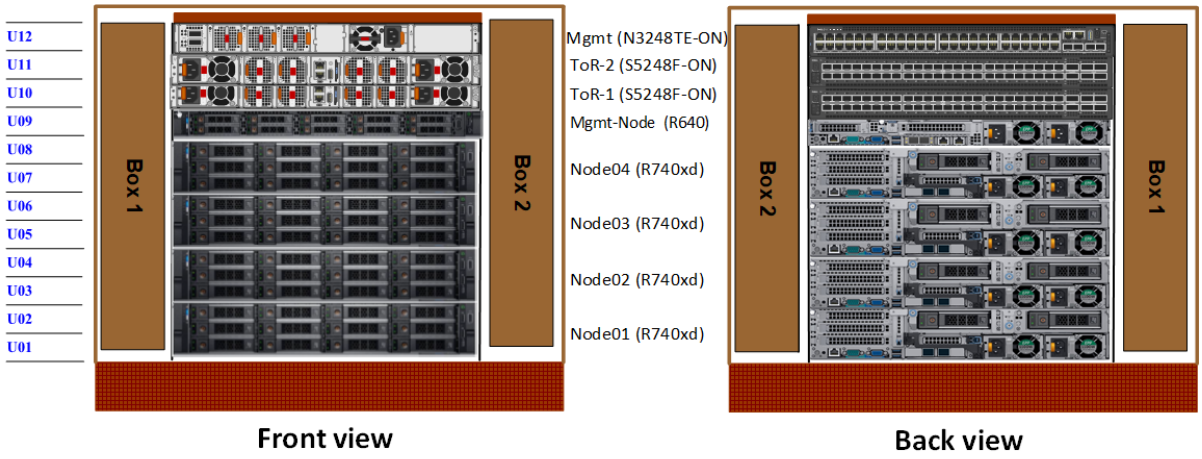

Figure 20. Dell Technologies four-node mini-transport rack for a hybrid unit

Dell Technologies service installs the components into the customer-provided rack before completing the deployment.

The following table lists the number of mini racks that are shipped based on the number of SUs that are ordered.

Table 27. Configuration mini-rack requirements

Dell Integrated System configuration	Required mini racks
4 nodes	1
8 nodes	2
12 nodes	3
16 nodes	4

The following figures show the switch and server placement for a 4-node minimum configuration up to a 16-node configuration. The solution comes pre-racked, stacked, and cabled, ready for a Dell Technologies Engineer to configure into your data center and to complete the deployment as an IaaS platform.

Additional Dell Technologies consulting services are available to help you tailor the solution.

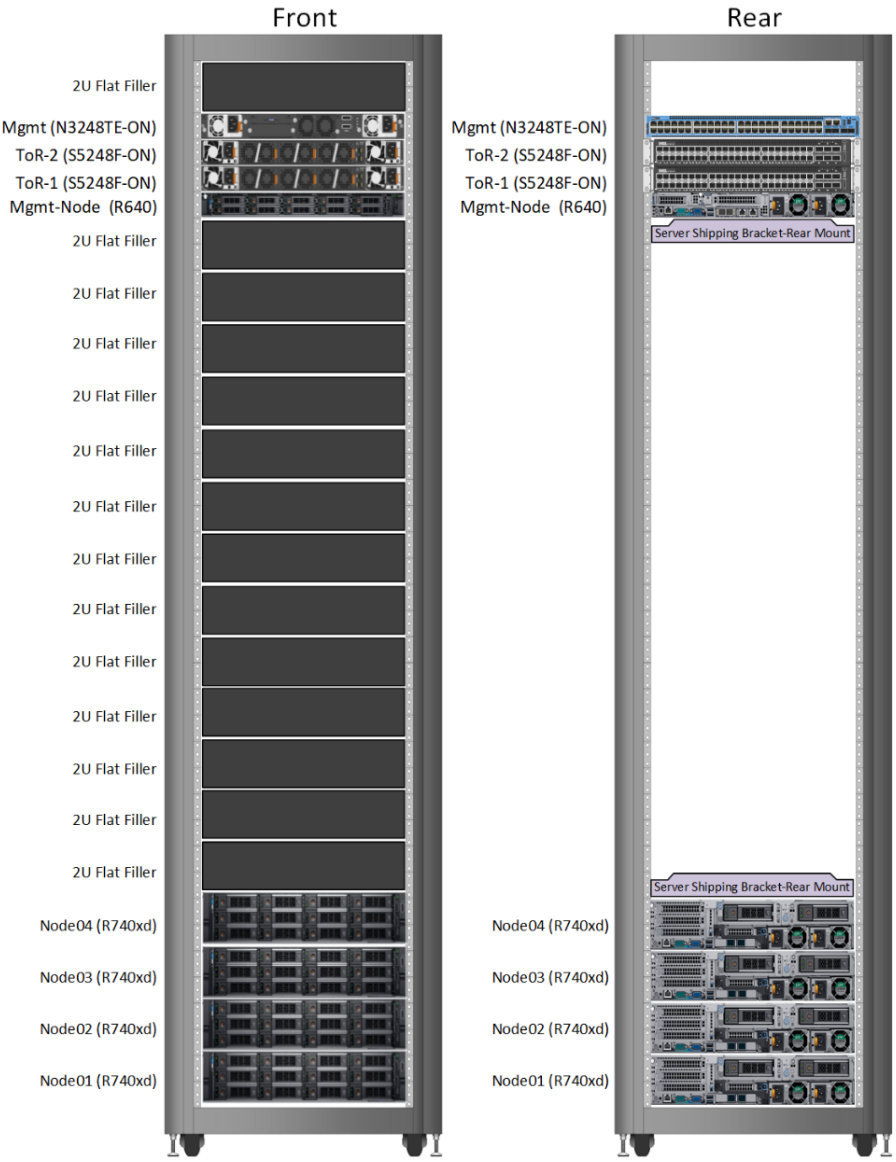

Figure 21. Minimum hybrid configuration elevation: 4-node SU

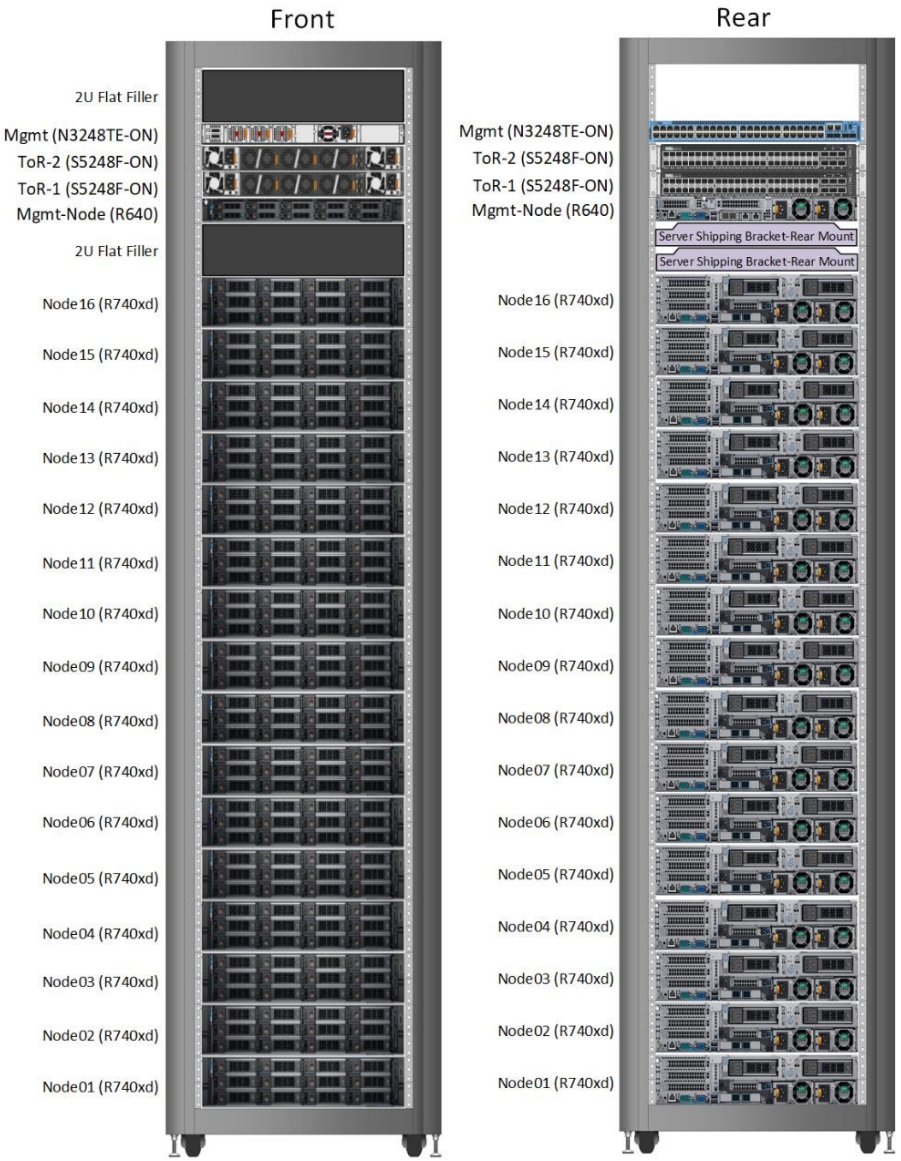

Figure 22. Maximum hybrid configuration elevation: 16-node SU

Supported PDU options

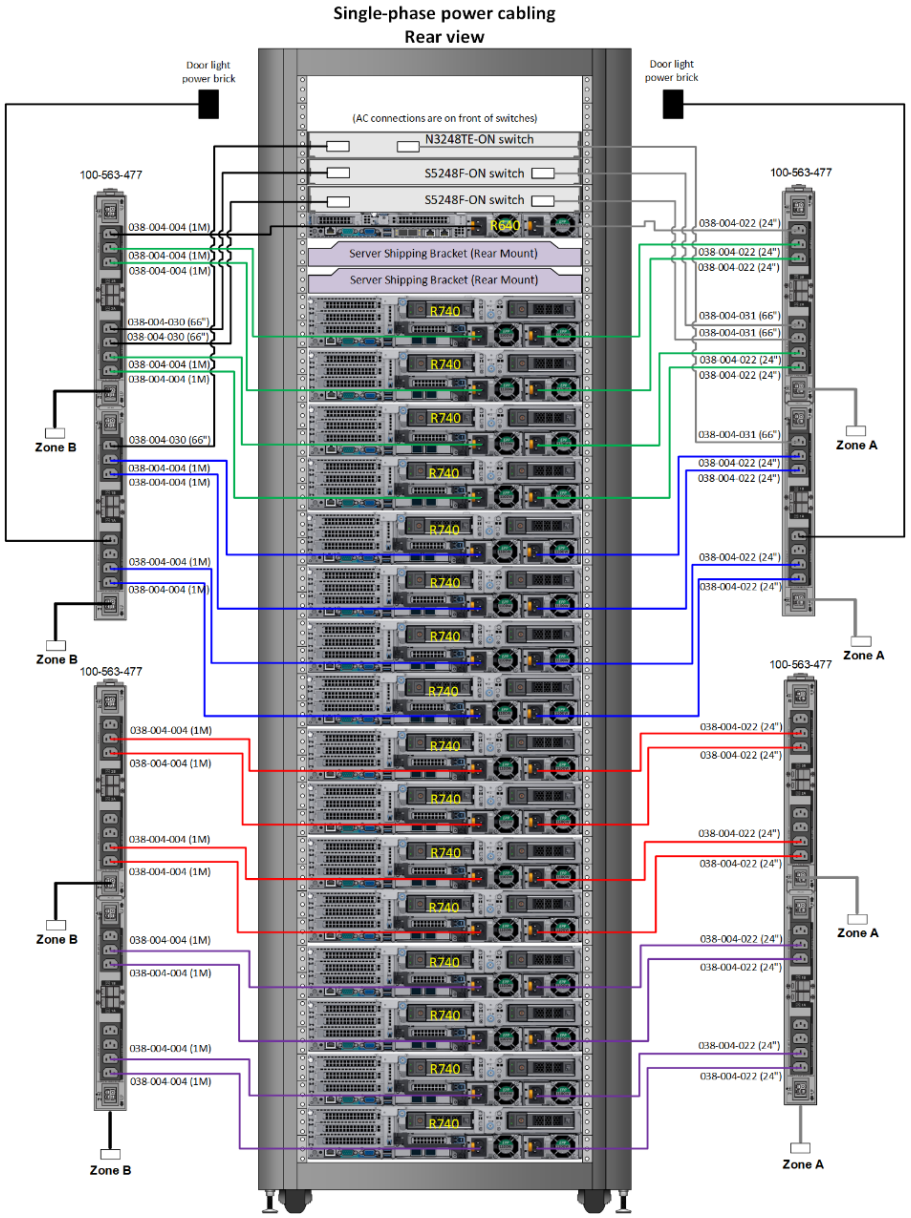

Figure 23. Hybrid configuration: Single phase PDU

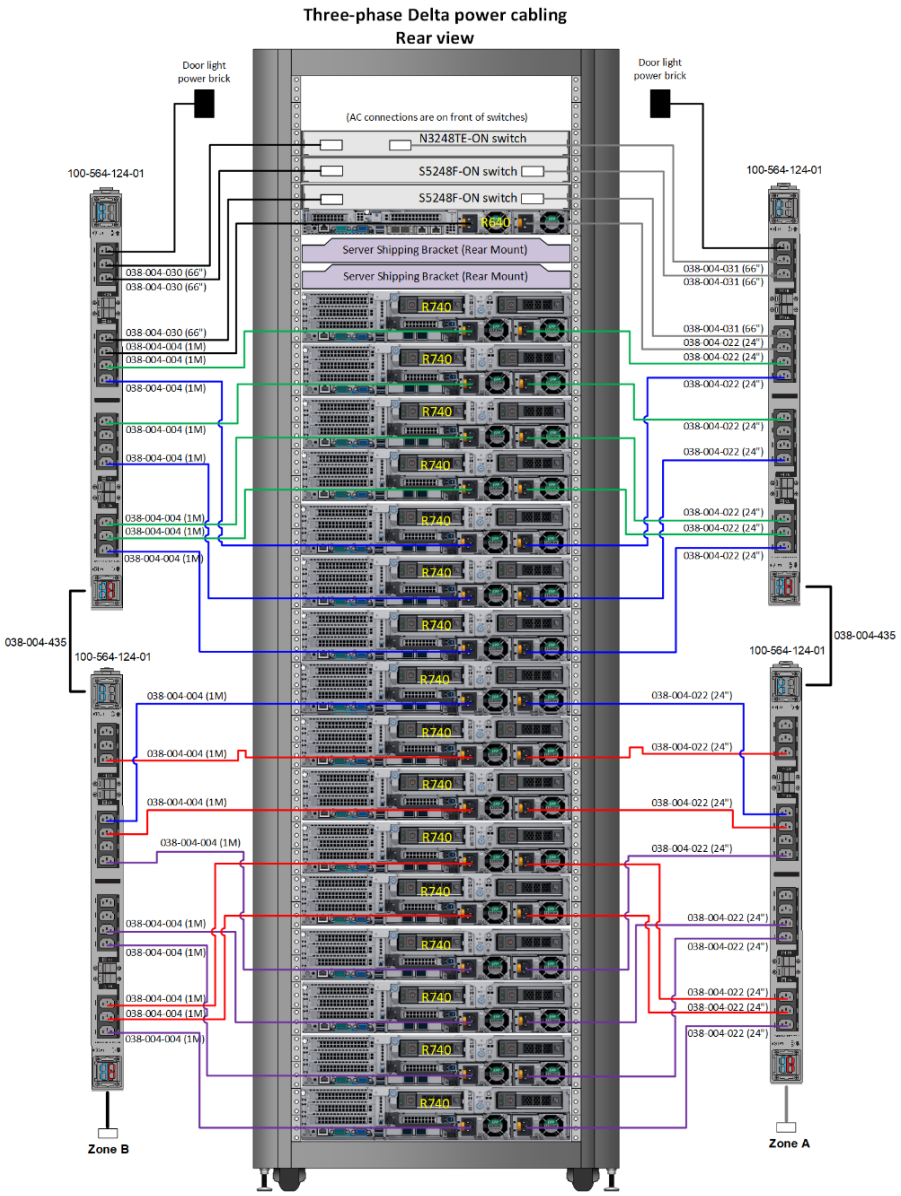

Figure 24. Hybrid configuration: Three-phase Delta PDU

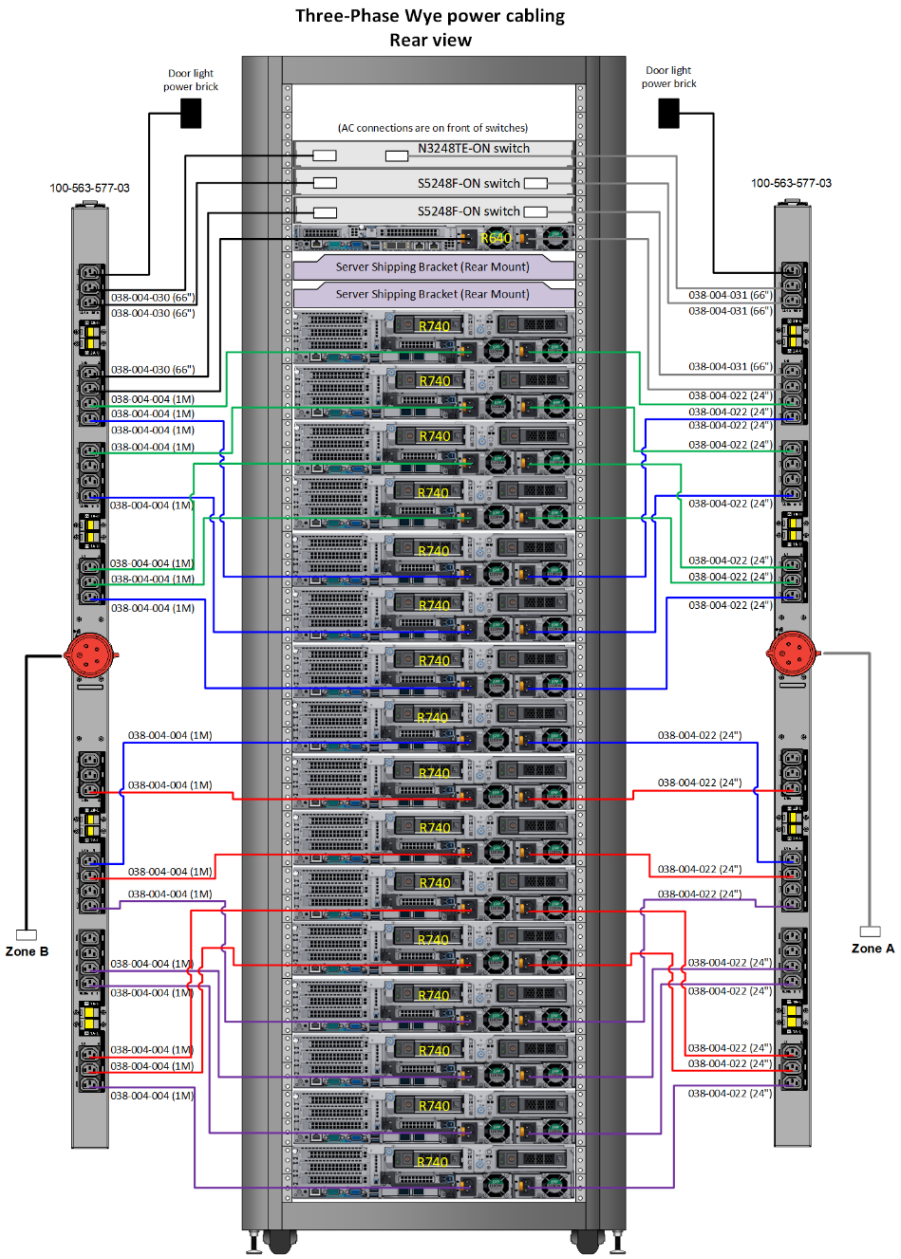

Figure 25. Hybrid configuration: Three-phase Wye PDU

All-flash scale-unit configuration

The Dell Integrated System all flash is also available pre-racked in a Dell Technologies rack and PDU. It can be ordered without the rack and PDU and integrated into a customer-provided dedicated rack and PDU.

NOTE: If you use a customer-provided rack and PDU, the customer must ensure that they have the required power and space for serviceability. For information, see c-environmental-requirements.

If you use a customer-provided rack and PDU, the customer must ensure that they have the required power and space for serviceability. For information, see c-environmental-requirements.

The following figures show switch and server placement for a minimum 4-node all-flash configuration up to 16-node all-flash configuration. The solution comes pre-racked, stacked, and cabled, ready for a Dell Technologies Engineer to configure into your data center and to complete the deployment as an IaaS platform.

Additional Dell Technologies consulting services are available to help you tailor the solution.

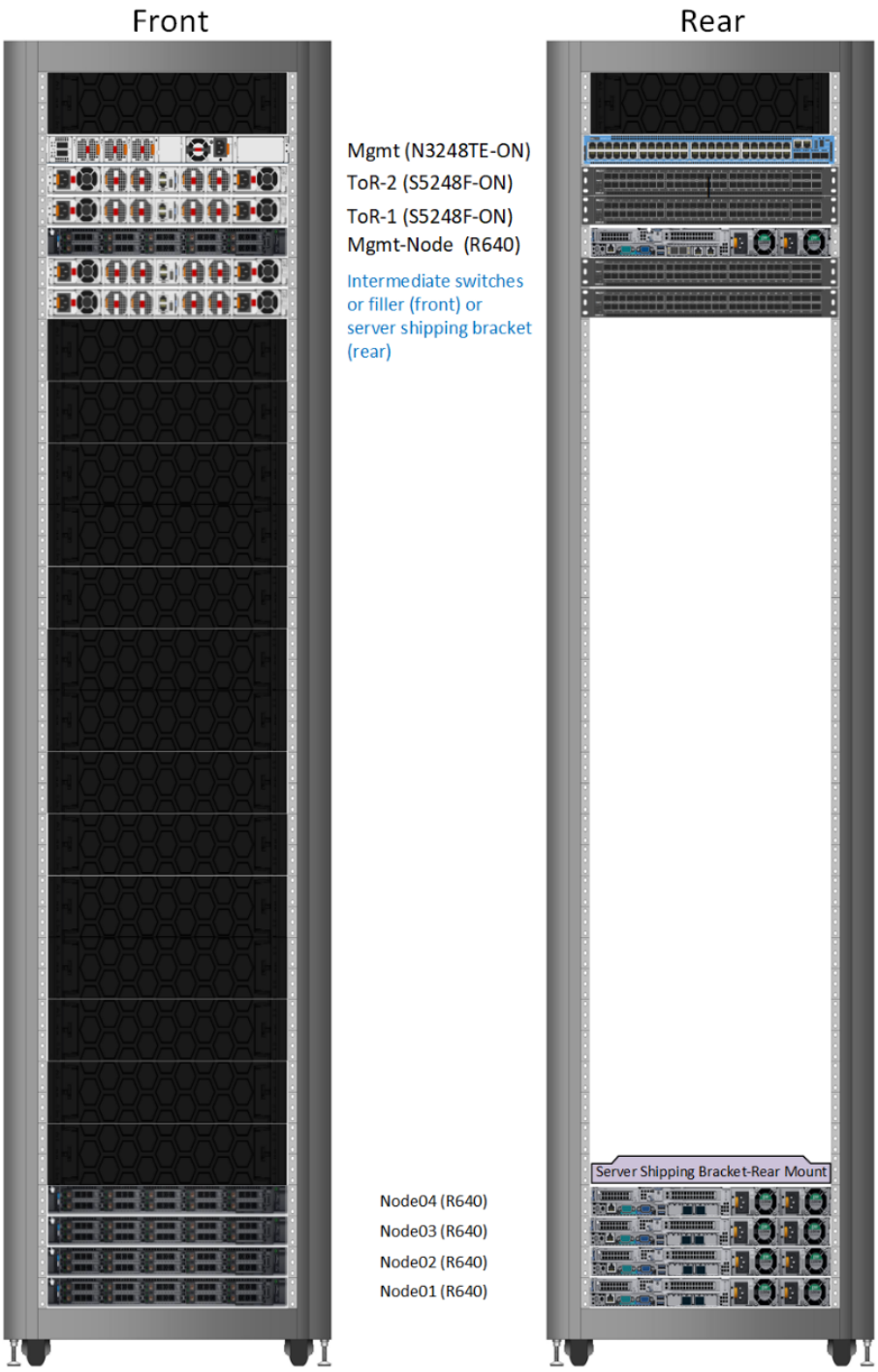

Figure 26. Minimum all-flash configuration elevation: 4-node SU

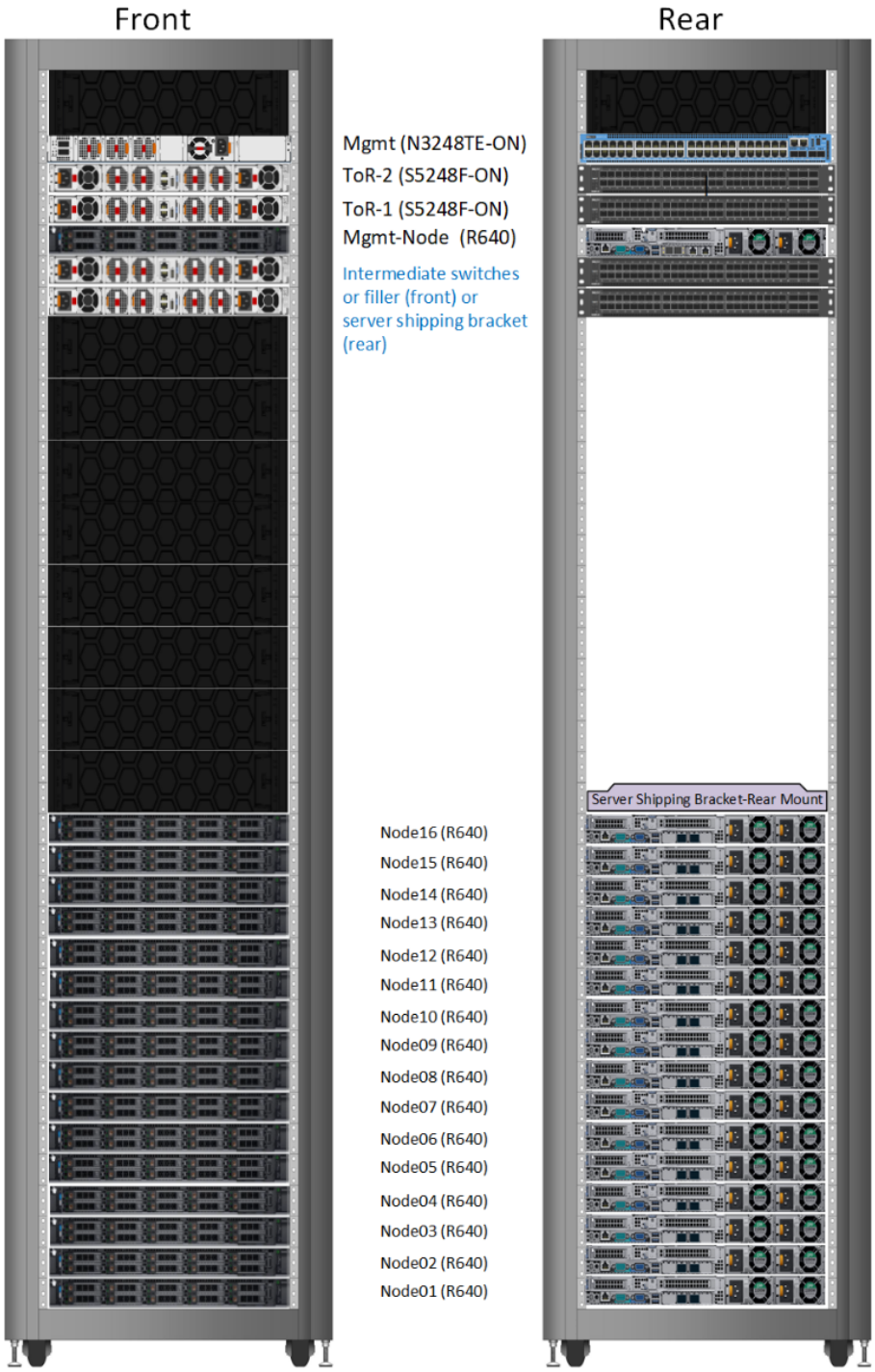

Figure 27. Maximum all-flash configuration elevation: 16-node SU

Supported PDU options

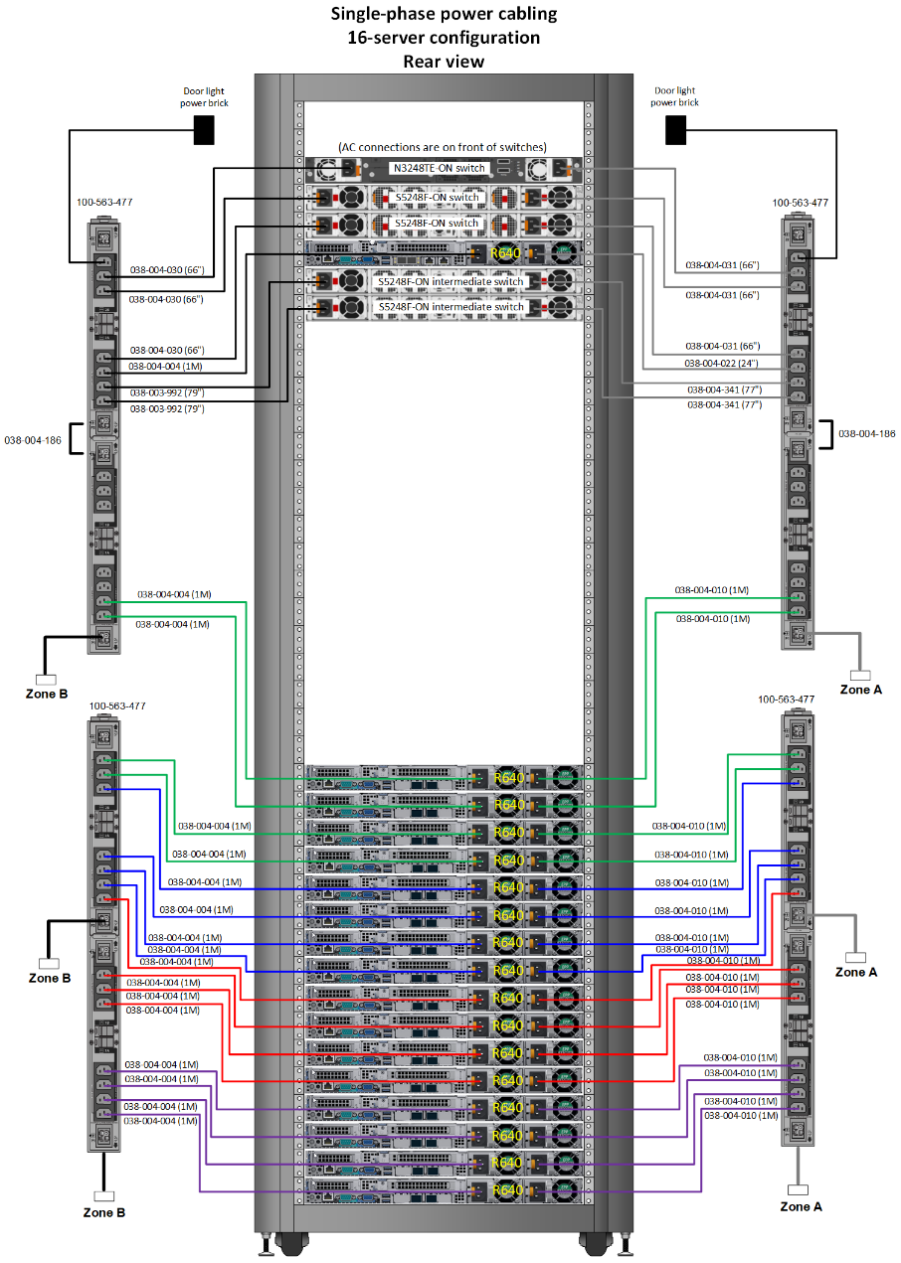

Figure 28. All-flash configuration: Single-phase PDU

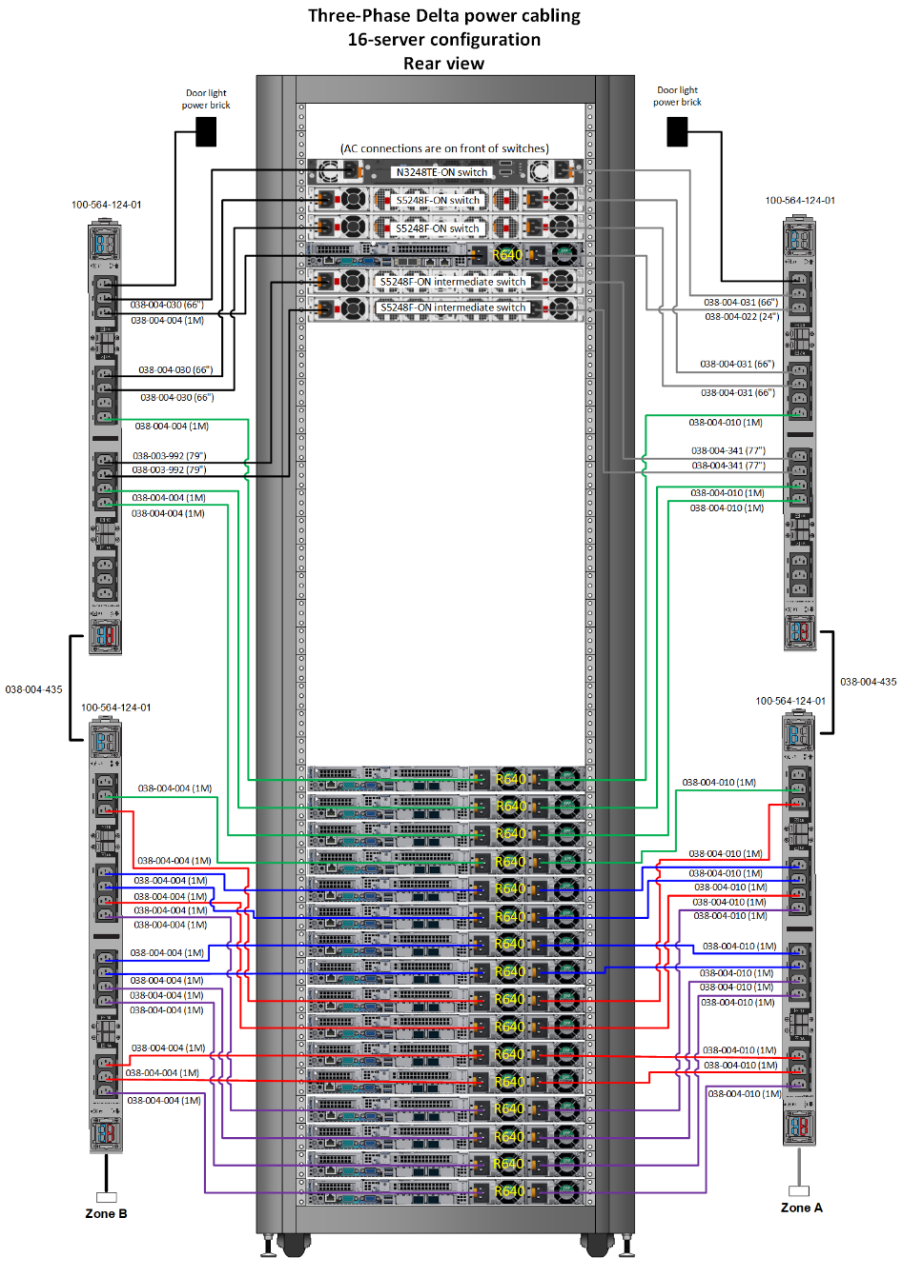

Figure 29. All-flash configuration: Three-phase Delta PDU

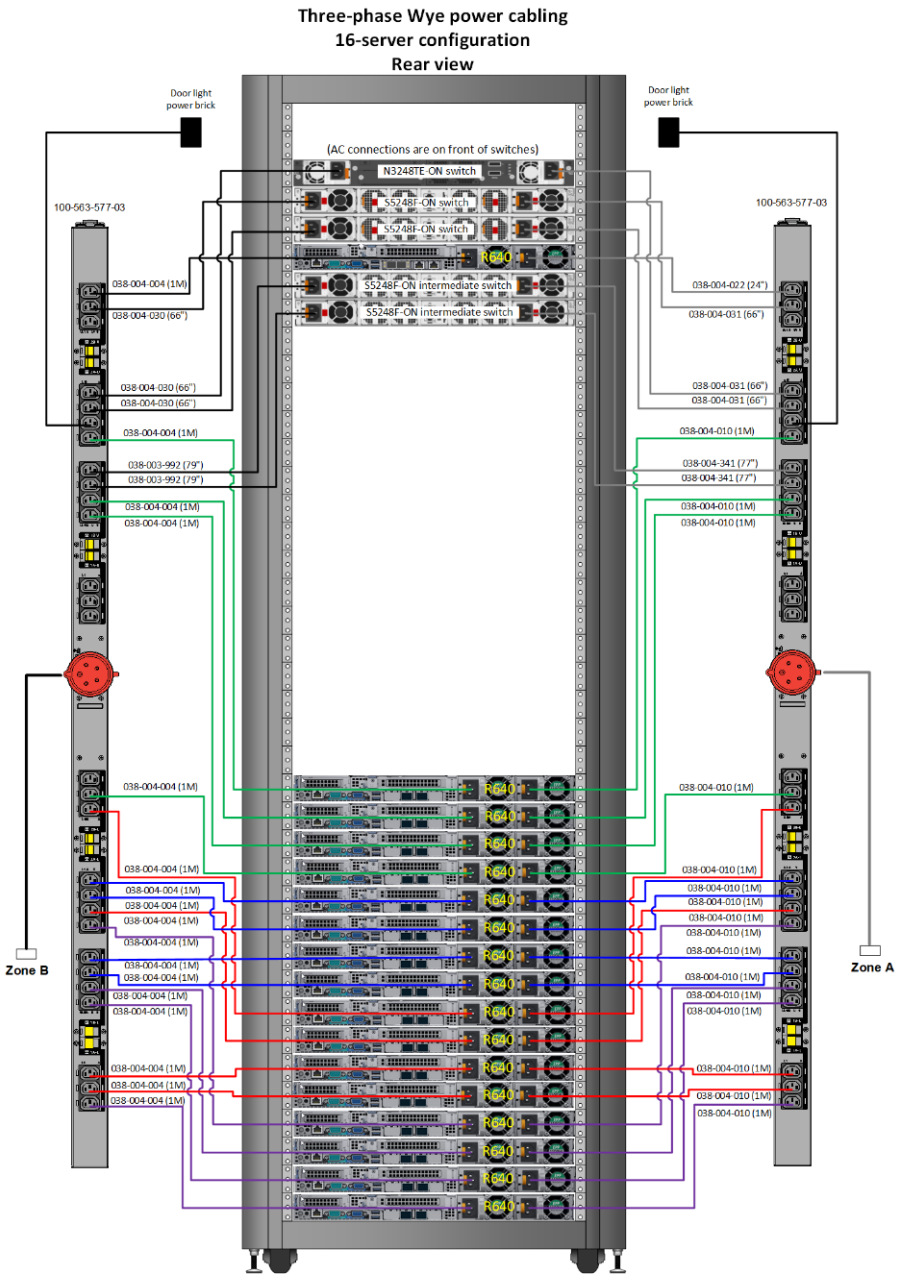

Figure 30. All-flash configuration: Three-phase Wye PDU

All-flash tactical configuration

Dell Integrated System for Microsoft Azure Stack Hub tactical is based on the Dell PowerEdge T-R640 all-flash configuration, which is modified into a ruggedized transit case as shown in the following figures.

Figure 31. Dell T-R640 in management transit case (front view and rear view)

Figure 32. Dell T-R640 in core transit case (front and rear view)

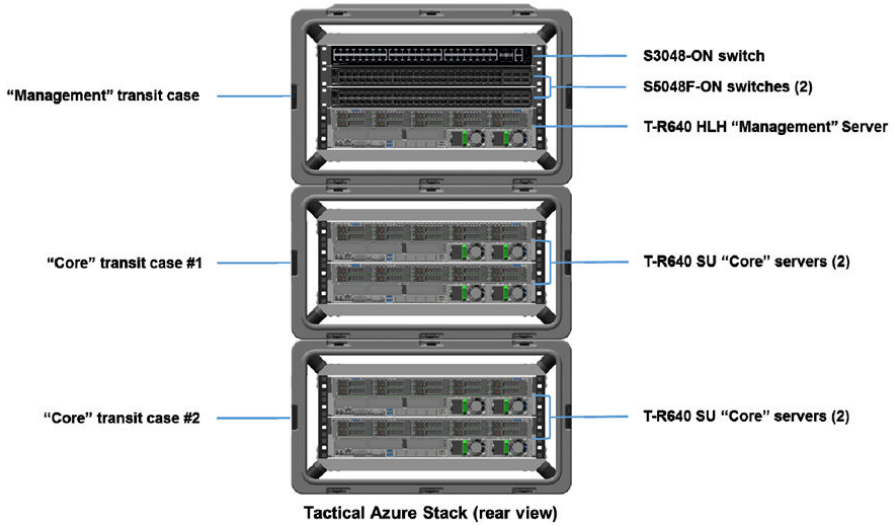

Figure 33. Dell Integrated System tactical (stacked rear view)

5

Networking and Cabling

Topics:

- Networking
- Scale unit node network connectivity
- Border connectivity
- Dense configuration networking
- Hybrid configuration networking
- All-flash configuration networking
- Azure Stack Hub switch cabling
- Border Gateway Protocol routing
- Static routing
- Transparent proxy
- Firewall integration
- Deployment

Networking

Overview

The following figure shows the Azure Stack Hub network topology.

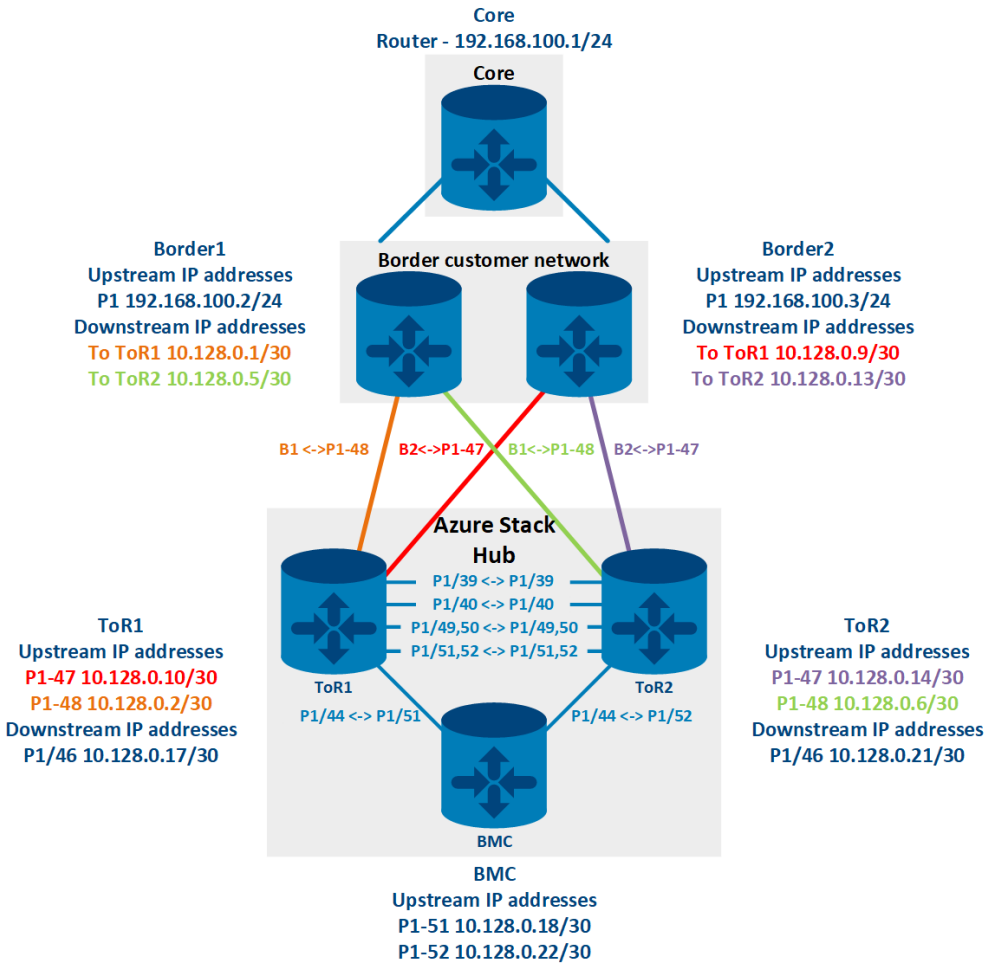

Figure 34. Azure Stack Hub network topology

Network transceivers

Dell Integrated System networking can use several transceiver types depending on customer network requirements. The following table lists the network transceivers that are supported for the solution.

NOTE: Uplink connections (from the ToR switches to a customer's edge devices) can employ the optical transceiver types that are listed in the following table. For the Cisco C93180YC-FX switch, only short-range 25 Gb SFP28+ optical transceivers have been validated.

Table 28. Supported network transceivers

SFP module	S5248F-ON ToR Hybrid and all-flash configurations	Cisco C93180YC-FX ToR All-flash configuration
10 GbE SR LC SFP+	Yes	No
10 GbE LR LC SFP+	Yes	No
25 GbE SR LC SFP28+	Yes	Yes
25 GbE LR LC SFP28+	Yes	No

NOTE: Cisco switch is only available with the customer-rack option. For details, see Rail kit information .

Scale unit node network connectivity

The following figure shows the scale unit node network connectivity for the server for either a hybrid, all flash, or dense configuration.

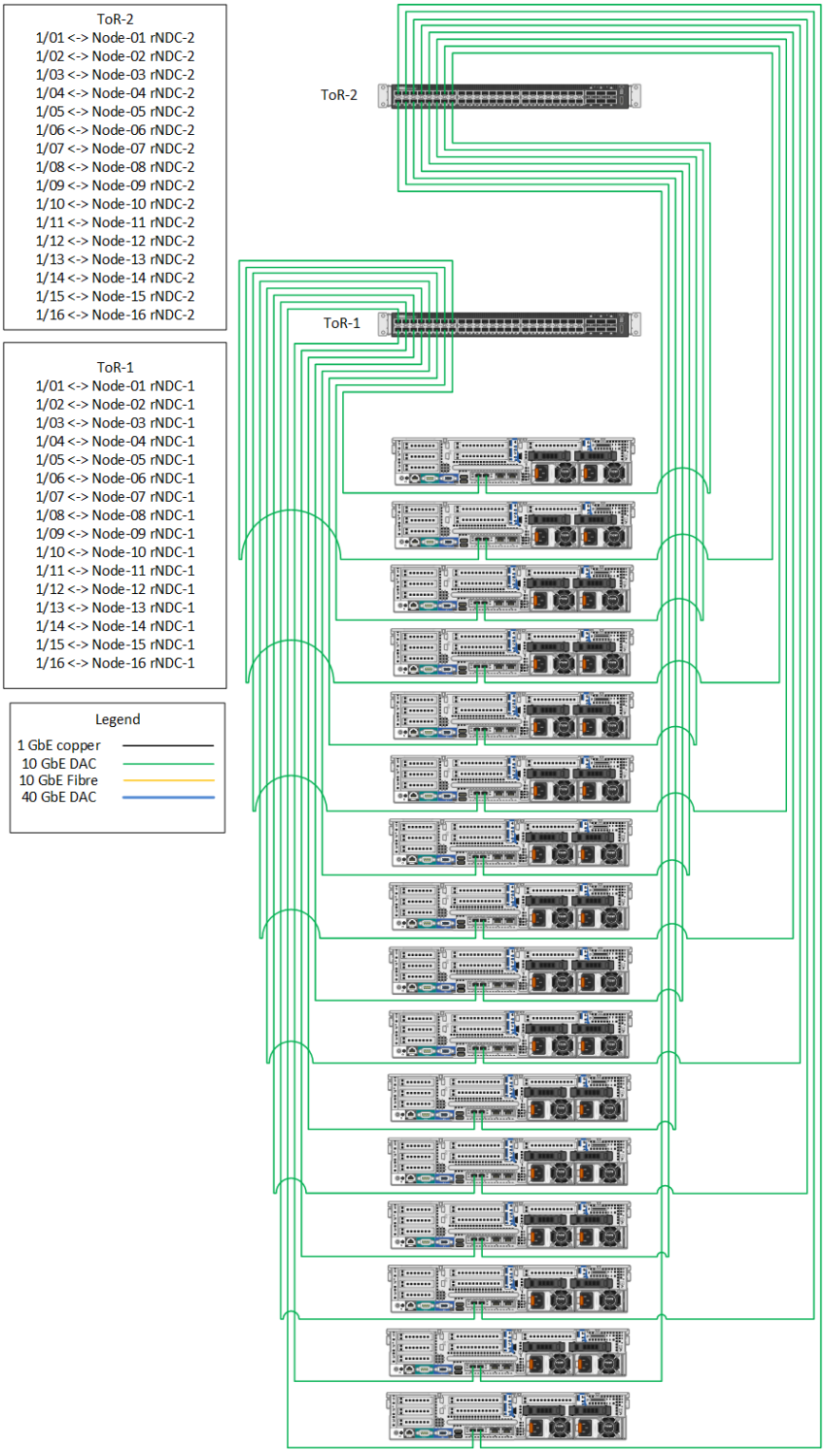

Figure 35. Scale unit node network connectivity

Border connectivity

Network integration planning is important for proper operation and management of the solution. Planning begins during the IP distribution when you choose whether to use dynamic routing with Border Gateway Protocol (BGP). This choice requires that you assign a 16-bit BGP autonomous system number (public or private) or use static routing, where Dell Technologies assigns a static default route to the border devices.

The following figure shows the border connectivity for the server for either a hybrid, all flash, or dense configuration.

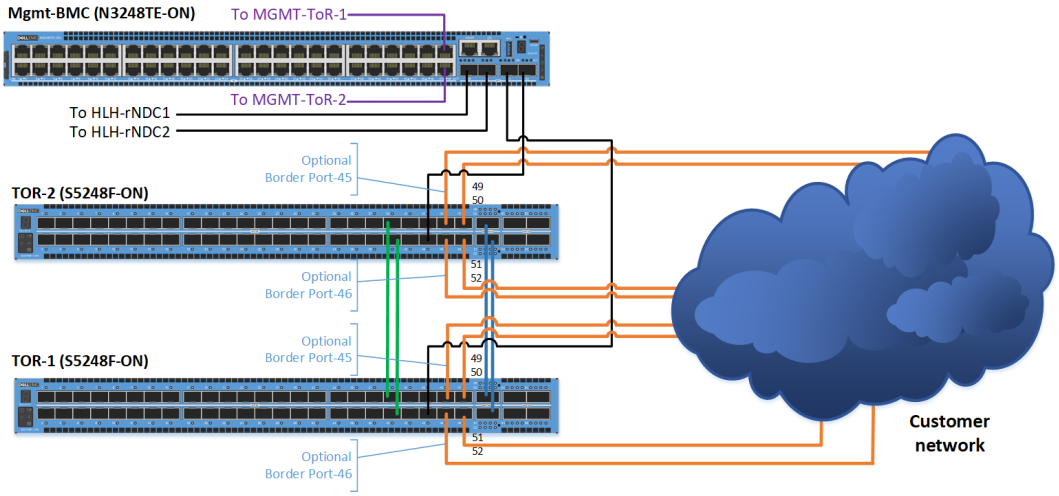

Figure 36. Border connectivity

Dense configuration networking

Server and switch port connections

The server and switch port connections are listed in Azure Stack Hub switch cabling.

HLH management network connectivity

The following figures show the HLH management network connectivity.

Figure 37. PowerEdge R640 server (rear view)

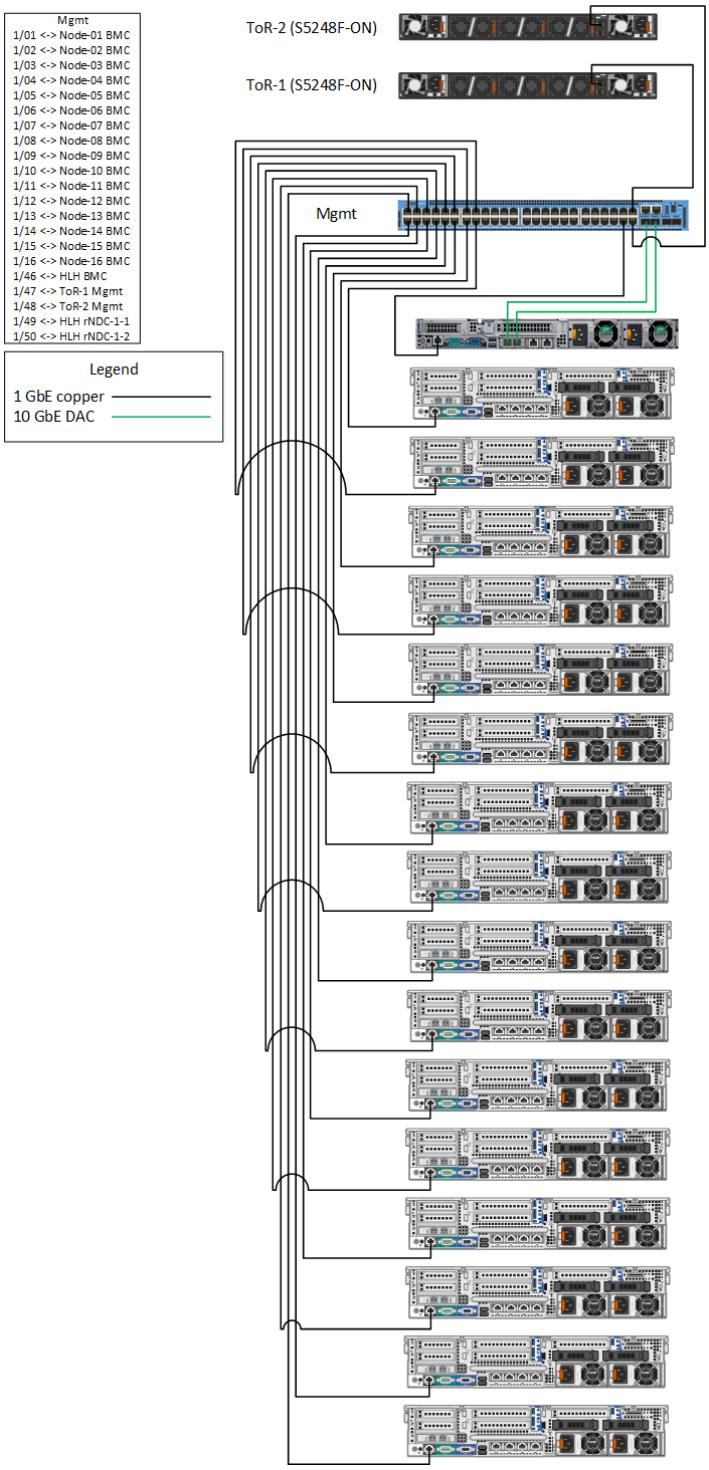

Figure 38. Dense configuration: HLH management network connectivity

Scale-unit node connectivity

The following figure shows the SU node connectivity for the PowerEdge R840 server for a dense configuration.

Figure 39. PowerEdge R840 server (rear view)

Hybrid configuration networking

Server and switch port connections

The server and switch port connections are listed in Azure Stack Hub switch cabling.

HLH management network connectivity

The following figures show the HLH management network connectivity for a hybrid configuration.

Figure 40. PowerEdge R640 server (rear view)

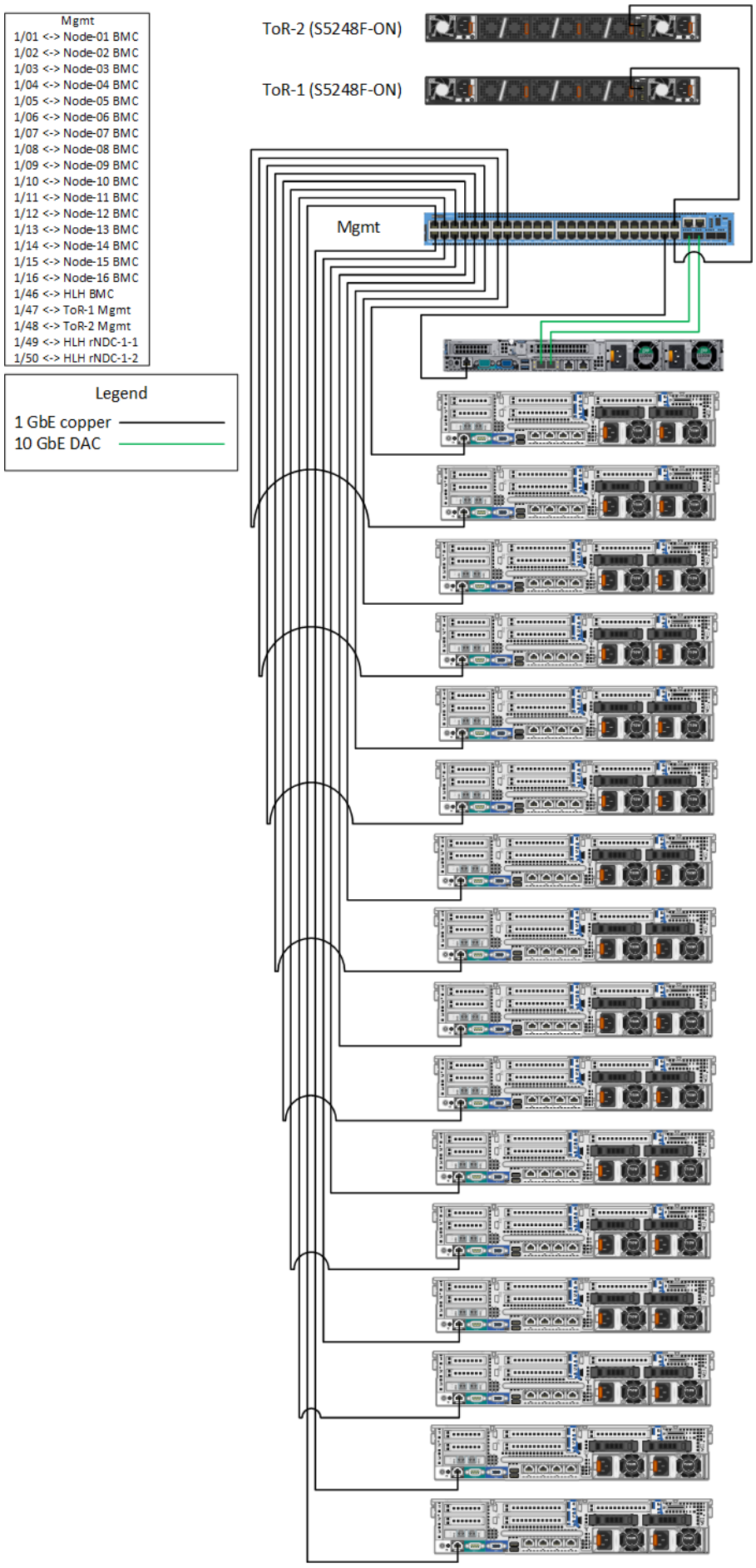

Figure 41. Hybrid configuration: HLH management network connectivity

Scale-unit node connectivity

The following figure shows the SU node connectivity for the PowerEdge R740xd server for a hybrid configuration.

Figure 42. PowerEdge R740xd server (rear view)

All-flash configuration networking

Server and switch port connections

The server and switch port connections are listed in Azure Stack Hub switch cabling.

HLH management network connectivity

The following figures show the HLH management network connectivity for an all-flash configuration.

Figure 43. PowerEdge R640 HLH server (rear view)

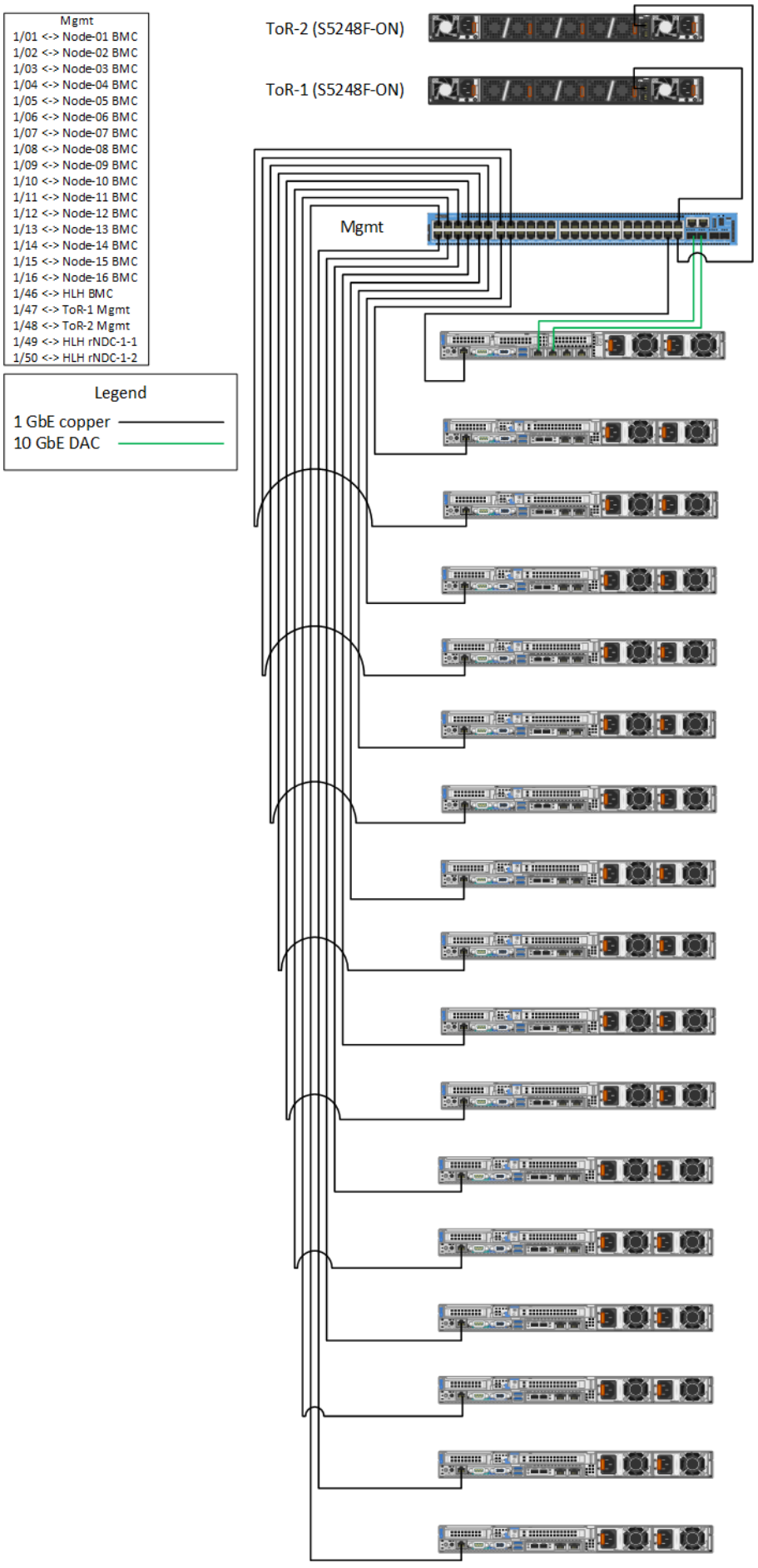

Figure 44. All-flash configuration: HLH management network connectivity

Scale-unit node connectivity

The following figure shows the SU node connectivity for the PowerEdge R640 server for an all-flash configuration.

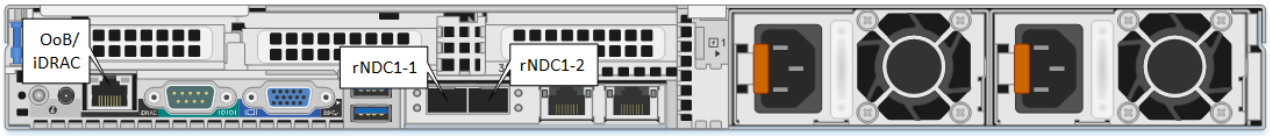

Figure 45. PowerEdge R640 server (rear view)

Azure Stack Hub switch cabling

The following tables list the port maps for the baseboard management controller (BMC) switch, also called the management switch, and the top-of-rack (ToR) switches.

Server and switch port description references

This list defines the server and switch port connections that are listed in the tables in the following sections.

- **GMTP**—Management ports on ToR switch (PowerSwitch S5248F-ON)
- **BMC**—Management switch (PowerSwitch N3248TE-ON)
- **HLH**—Hardware life cycle host (PowerEdge R640)
- **OoB**—Connects to iDRAC management ports
- **rNDC1**—Left port on Mellanox Connectx-4
- **rNDC2**—Right port on Mellanox Connectx-4
- **HLH-rNDC1**—Left port on Intel NDC card

N3248TE-ON BMC port map

The following table lists the connection and cable types, node ports, and switch ports for the N3248TE-ON BMC switch for the hybrid, all-flash, and dense configurations.

Table 29. N3248TE-ON BMC connection and cable types, node ports, and switch ports

Connection and cable type	From originating port	To BMC switch port
1 Gb Cat 6	Node 01 OoB NIC (iDRAC)	Port 01
1 Gb Cat 6	Node 02 OoB NIC (iDRAC)	Port 02
1 Gb Cat 6	Node 03 OoB NIC (iDRAC)	Port 03
1 Gb Cat 6	Node 04 OoB NIC (iDRAC)	Port 04
1 Gb Cat 6	Node 05 OoB NIC (iDRAC)	Port 05
1 Gb Cat 6	Node 06 OoB NIC (iDRAC)	Port 06
1 Gb Cat 6	Node 07 OoB NIC (iDRAC)	Port 07
1 Gb Cat 6	Node 08 OoB NIC (iDRAC)	Port 08
1 Gb Cat 6	Node 09 OoB NIC (iDRAC)	Port 09
1 Gb Cat 6	Node 10 OoB NIC (iDRAC)	Port 10
1 Gb Cat 6	Node 11 OoB NIC (iDRAC)	Port 11
1 Gb Cat 6	Node 12 OoB NIC (iDRAC)	Port 12
1 Gb Cat 6	Node 13 OoB NIC (iDRAC)	Port 13

Table 29. N3248TE-ON BMC connection and cable types, node ports, and switch ports (continued)

1 Gb Cat 6	Node 14 OoB NIC (iDRAC)	Port 14
1 Gb Cat 6	Node 15 OoB NIC (iDRAC)	Port 15
1 Gb Cat 6	Node 16 OoB NIC (iDRAC)	Port 16
1 Gb Cat 6	BMC reserved PDU	Port 41
1 Gb Cat 6	BMC reserved PDU	Port 42
1 Gb Cat 6	BMC reserved PDU	Port 43
1 Gb Cat 6	BMC reserved PDU	Port 44
1 Gb Cat 6	Hardware Lifecycle Host OoB NIC (iDRAC)	Port 46
1 Gb Cat 6	ToR 1 switch management port	Port 47
1 Gb Cat 6	ToR 2 switch management port	Port 48
10 Gb SFP28-Twinaxial	Hardware Lifecycle Host 10 GbE port 1 (PCI1-1)	Port 49
10 Gb SFP28-Twinaxial	Hardware Lifecycle Host 10 GbE port 2 (PCI1-2)	Port 50
10 Gb SFP28-Twinaxial	S5248F-ON ToR 1 switch port 44	Port 51
10 Gb SFP28-Twinaxial	S5248F-ON ToR 2 switch port 44	Port 52

S5248F-ON ToR 1 port map

The following table lists the connection and cable types, node ports, and switch ports for the S5248F-ON ToR 1 switch for the hybrid, all-flash, and dense configurations.

Table 30. S5248F-ON ToR 1 connection and cable types, node ports, and switch ports

Connection and cable type	From originating port	To ToR 1 switch port
25 Gb Twinaxial	Node 01 NIC port 1 (rNDC1-1)	Port 01
25 Gb Twinaxial	Node 02 NIC port 1 (rNDC1-1)	Port 02
25 Gb Twinaxial	Node 03 NIC port 1 (rNDC1-1)	Port 03
25 Gb Twinaxial	Node 04 NIC port 1 (rNDC1-1)	Port 04
25 Gb Twinaxial	Node 05 NIC port 1 (rNDC1-1)	Port 05
25 Gb Twinaxial	Node 06 NIC port 1 (rNDC1-1)	Port 06
25 Gb Twinaxial	Node 07 NIC port 1 (rNDC1-1)	Port 07
25 Gb Twinaxial	Node 08 NIC port 1 (rNDC1-1)	Port 08
25 Gb Twinaxial	Node 09 NIC port 1 (rNDC1-1)	Port 09
25 Gb Twinaxial	Node 10 NIC port 1 (rNDC1-1)	Port 10
25 Gb Twinaxial	Node 11 NIC port 1 (rNDC1-1)	Port 11
25 Gb Twinaxial	Node 12 NIC port 1 (rNDC1-1)	Port 12
25 Gb Twinaxial	Node 13 NIC port 1 (rNDC1-1)	Port 13
25 Gb Twinaxial	Node 14 NIC port 1 (rNDC1-1)	Port 14

Table 30. S5248F-ON ToR 1 connection and cable types, node ports, and switch ports (continued)

25 Gb Twinaxial	Node 15 NIC port 1 (rNDC1-1)	Port 15
25 Gb Twinaxial	Node 16 NIC port 1 (rNDC1-1)	Port 16
25 Gb Twinaxial	ToR 2 switch port 39 (BGP)	Port 39
25 Gb Twinaxial	ToR 2 switch port 40 (BGP)	Port 40
10 Gb Twinaxial	BMC switch port 51	Port 44
25 Gb Fiber	Customer border switch 4 (optional)	Port 45
25 Gb Fiber	Customer border switch 3 (optional)	Port 46
25 Gb Fiber	Customer border switch 2	Port 47
25 Gb Fiber	Customer border switch 1	Port 48
200 Gb Twinaxial	ToR2 VLTi peer link	Port 49/50
200 Gb Twinaxial	ToR2 VLTi peer link	Port 51/52

NOTE: Ports 49/50 and 50/51 on the S5248F-ON use a single jack that can be configured with either a single density QSFP for 100 Gb connectivity or a double density QSFP for 200 Gb connectivity.

The standard shipping configuration is to have QSFP-DD cables running between the two ToRs for 200 GB connectivity. On the switches, the differences between using the 100 Gb single-density cables and the 200 Gb double-density cables is shown in the following tables.

Table 31. Single-density cables - 100 GB

Port	Status	Speed	Duplex
Eth 1/1/49	Up	100 Gb	Full
Eth 1/1/50	Down	0	Full
Eth 1/1/51	Up	100 Gb	Full
Eth 1/1/52	Down	0	Full

Table 32. Double-density cables - 200 GB

Port	Status	Speed	Duplex
Eth 1/1/49	Up	100 Gb	Full
Eth 1/1/50	Up	100 Gb	Full
Eth 1/1/51	Up	100 Gb	Full
Eth 1/1/52	Up	100 Gb	Full

S5248F-ON ToR 2 port map

The following table lists the connection and cable types, node ports, and switch ports for the S5248F-ON ToR 2 switch for the hybrid, all-flash, and dense configurations.

Table 33. S5248F-ON ToR 2 connection and cable types, node ports, and switch ports

Connection and cable type	From originating port	To switch port
25 Gb Twinaxial	Node 01 NIC port 2 (rNDC2-2)	Port 01
25 Gb Twinaxial	Node 02 NIC port 2 (rNDC2-2)	Port 02

Table 33. S5248F-ON ToR 2 connection and cable types, node ports, and switch ports (continued)

25 Gb Twinaxial	Node 03 NIC port 2 (rNDC2-2)	Port 03
25 Gb Twinaxial	Node 04 NIC port 2 (rNDC2-2)	Port 04
25 Gb Twinaxial	Node 05 NIC port 2 (rNDC2-2)	Port 05
25 Gb Twinaxial	Node 06 NIC port 2 (rNDC2-2)	Port 06
25 Gb Twinaxial	Node 07 NIC port 2 (rNDC2-2)	Port 07
25 Gb Twinaxial	Node 08 NIC port 2 (rNDC2-2)	Port 08
25 Gb Twinaxial	Node 09 NIC port 2 (rNDC2-2)	Port 09
25 Gb Twinaxial	Node 10 NIC port 2 (rNDC2-2)	Port 10
25 Gb Twinaxial	Node 11 NIC port 2 (rNDC2-2)	Port 11
25 Gb Twinaxial	Node 12 NIC port 2 (rNDC2-2)	Port 12
25 Gb Twinaxial	Node 13 NIC port 2 (rNDC2-2)	Port 13
25 Gb Twinaxial	Node 14 NIC port 2 (rNDC2-2)	Port 14
25 Gb Twinaxial	Node 15 NIC port 2 (rNDC2-2)	Port 15
25 Gb Twinaxial	Node 16 NIC port 2 (rNDC2-2)	Port 16
25 Gb Twinaxial	ToR 1 port 39 (BGP)	Port 39
25 Gb Twinaxial	ToR 1 port 40 (BGP)	Port 40
10 Gb Twinaxial	BMC port 52	Port 44
25 Gb Fiber	Customer border switch 4 (optional)	Port 45
25 Gb Fiber	Customer border switch 3 (optional)	Port 46
25 Gb Fiber	Customer border switch 2	Port 47
25 Gb Fiber	Customer border switch 1	Port 48
200 Gb Twinaxial	ToR 1 VLTi peer link	Port 49/50
200 Gb Twinaxial	ToR 1 VLTi peer link	Port 51/52

NOTE: Ports 49/50 and 50/51 on the S5248F-ON use a single jack that can be configured with either a single density QSFP for 100 Gb connectivity or a double density QSFP for 200 Gb connectivity.

The standard shipping configuration is to have QSFP-DD cables running between the two ToRs for 200 GB connectivity. On the switches, the differences between using the 100 Gb single-density cables and the 200 Gb double-density cables is shown in the following tables.

Table 34. Single-density cables - 100 Gb

Port	Status	Speed	Duplex
Eth 1/1/49	Up	100 Gb	Full
Eth 1/1/50	Down	0	Full
Eth 1/1/51	Up	100 Gb	Full
Eth 1/1/52	Down	0	Full

Table 35. Double-density cables - 200 Gb

Port	Status	Speed	Duplex

Table 35. Double-density cables - 200 Gb (continued)

Eth 1/1/49	Up	100 Gb	Full
Eth 1/1/50	Up	100 Gb	Full
Eth 1/1/51	Up	100 Gb	Full
Eth 1/1/52	Up	100 Gb	Full

The following table lists Cisco cable placement and port mapping.

NOTE: Cisco switch is only available with the customer-rack option. For details, see Rail kit information .

Table 36. Cisco cable placement and port mapping

Cisco C93180YC-FX					**Cisco 9348GC-FXP**		
Cable type	Originating port	ToR-1 switch port	Originating port	ToR-2 switch port	Cable type	Originating port	BMC switch port
25 GB Twinax	Node-01 – rNDC1-1	Port-01	Node-01 – rNDC2-2	Port-01	1 GB CAT6	Node-01– iDRAC	Port-01
	Node-02 – rNDC1-1	Port-02	Node-02 – rNDC2-2	Port-02		Node-02– iDRAC	Port-02
	Node-03 – rNDC1-1	Port-03	Node-03 – rNDC2-2	Port-03		Node-03– iDRAC	Port-03
	Node-04 – rNDC1-1	Port-04	Node-04 – rNDC2-2	Port-04		Node-04– iDRAC	Port-04
	Node-05 – rNDC1-1	Port-05	Node-05 – rNDC2-2	Port-05		Node-05– iDRAC	Port-05
	Node-06 – rNDC1-1	Port-06	Node-06 – rNDC2-2	Port-06		Node-06– iDRAC	Port-06
	Node-07 – rNDC1-1	Port-07	Node-07 – rNDC2-2	Port-07		Node-07– iDRAC	Port-07
	Node-08 – rNDC1-1	Port-08	Node-08 – rNDC2-2	Port-08		Node-08– iDRAC	Port-08
	Node-09 – rNDC1-1	Port-09	Node-09 – rNDC2-2	Port-09		Node-09– iDRAC	Port-09
	Node-10 – rNDC1-1	Port-10	Node-10 – rNDC2-2	Port-10		Node-10– iDRAC	Port-10
	Node-11 – rNDC1-1	Port-11	Node-11 – rNDC2-2	Port-11		Node-11– iDRAC	Port-11
	Node-12 – rNDC1-1	Port-12	Node-12 – rNDC2-2	Port-12		Node-12– iDRAC	Port-12
	Node-13 – rNDC1-1	Port-13	Node-13 – rNDC2-2	Port-13		Node-13– iDRAC	Port-13
	Node-14 – rNDC1-1	Port-14	Node-14 – rNDC2-2	Port-14		Node-14– iDRAC	Port-14
	Node-15 – rNDC1-1	Port-15	Node-15 – rNDC2-2	Port-15		Node-15– iDRAC	Port-15
	Node-16 – rNDC1-1	Port-16	Node-16 – rNDC2-2	Port-16		Node-16– iDRAC	Port-16
	ToR-2	Port-39	ToR-1	Port-39		HLH-iDRAC	Port-46

Table 36. Cisco cable placement and port mapping (continued)

	Switch Port-39		Switch Port-39				
	ToR-2 Switch Port-40	Port-40	ToR-1 Switch Port-40	Port-40		ToR-1 Switch MGMT	Port-47
	BMC Switch Port-51	Port-44	BMC Switch Port-52	Port-44		ToR-2 Switch MGMT	Port-48
10/25 GB Fiber	Customer Border-4 (optional)	Port-45	Customer Border-4 (optional)	Port-45	10/25 GbE Twinax	HLH-PCI1-1	Port-49
	Customer Border-3 (optional)	Port-46	Customer Border-3 (optional)	Port-46		HLH-PCI1-2	Port-50
	Customer Border-2	Port-47	Customer Border-2	Port-47	25 GbE Twinax	ToR-1 Port-44	Port-51
	Customer Border-1	Port-48	Customer Border-1	Port-48		ToR-2 Port-44	Port-52
40/100 GB Twinax	ToR-2 Port-49	Port-49	ToR-1 Port-49	Port-49			
	ToR-2 Port-50	Port-50	ToR-1 Port-50	Port-50			

Border Gateway Protocol routing

Using a dynamic routing protocol such as BGP guarantees that your system is always aware of network changes and facilitates administration.

As shown in the following figure, you can restrict advertising the private IP space on the ToR by using a prefix list that denies the private IP subnets. You can apply the prefix list as a route map on the connection between the ToR and the border.

The Software Load Balancer (SLB) running in the Dell Integrated System peers to the ToR devices so that the SLB can dynamically advertise VIP addresses.

To ensure that user traffic immediately and transparently recovers from failure, configure the virtual private cloud (VPC) or multi-chassis link aggregation (MLAG) between the ToR devices. This configuration enables MLAG use to the hosts, and hot standby router protocol (HSRP) or virtual router redundancy protocol (VRRP) that provides network redundancy for the IP networks.

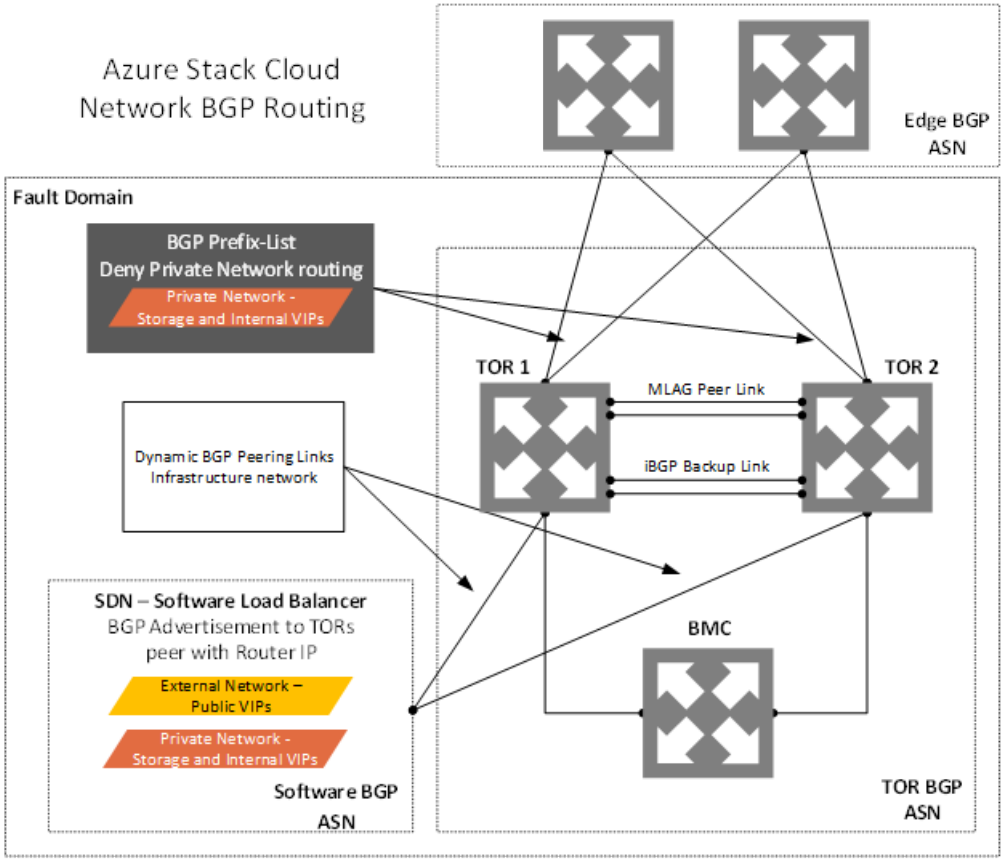

Figure 46. BGP routing for Microsoft Azure Stack Hub cloud network

Static routing

Using static routes adds more fixed configuration to the border and to ToR devices. Static routes require thorough analysis before you make any change. Issues that are caused by a configuration error might take more time to roll back depending on the changes you made. We do not recommend static routing, but it is supported.

To integrate Microsoft Azure Stack Hub into your networking environment by using this method, the border device must be configured with static routes pointing to the ToR devices for traffic that is destined for external networks or public VIPs.

Configure the ToR devices with a static default route that sends all traffic to the border devices. The one traffic exception to this rule is for the private space, which is blocked using an ACL that is applied on the ToR to the border connection.

The remaining configuration is the same as it is for BGP routing. The BGP dynamic routing is still used inside the rack. It is an essential tool for the SLB and other components and cannot be disabled or removed.

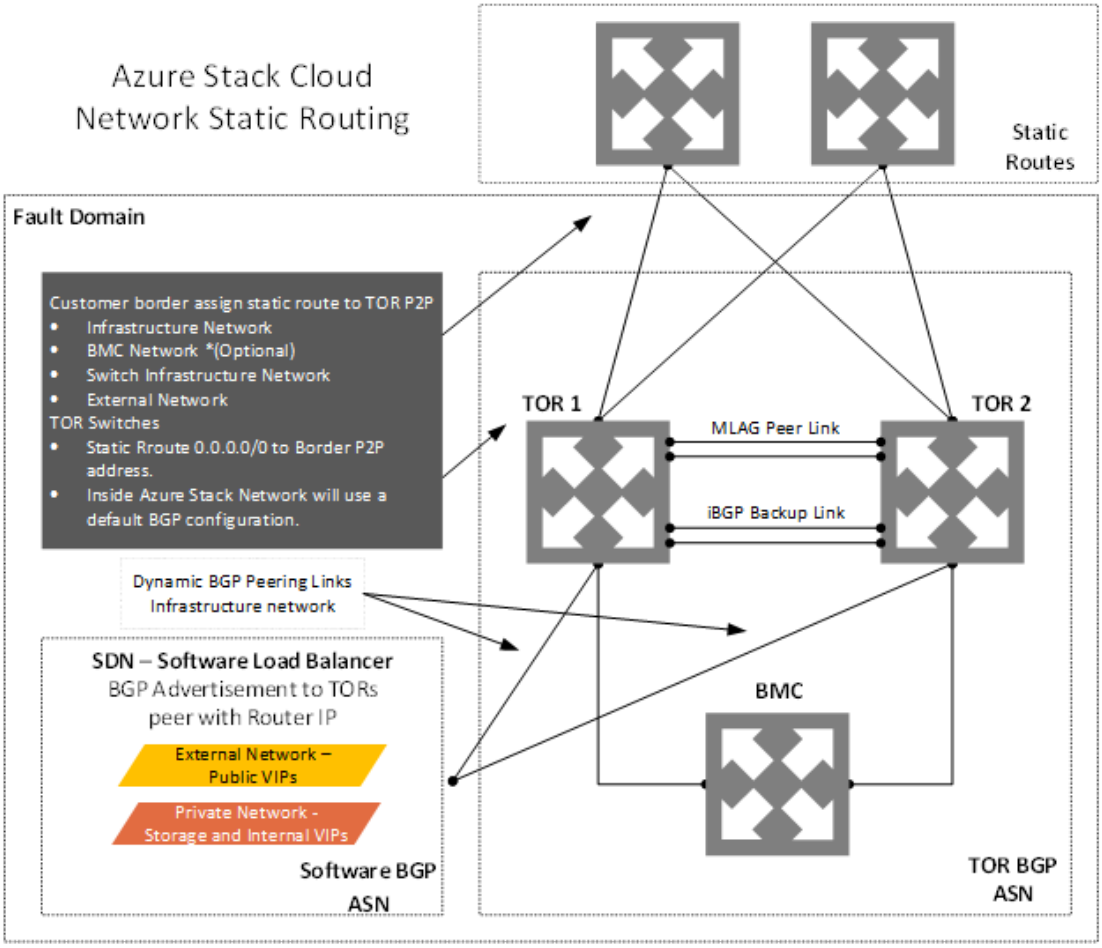

Figure 47. Static routing for Microsoft Azure Stack Hub cloud network

Transparent proxy

A transparent proxy (also known as an intercepting, inline, or forced proxy) intercepts normal communication at the network layer without requiring any special client configuration, as shown in the following figure. Customers do not need to be aware of the existence of the proxy.

The solution does not support normal proxies. If the data center requires all traffic to use a proxy, configure a transparent proxy to process all traffic from the rack to handle it according to policy, separating between the zones on your network.

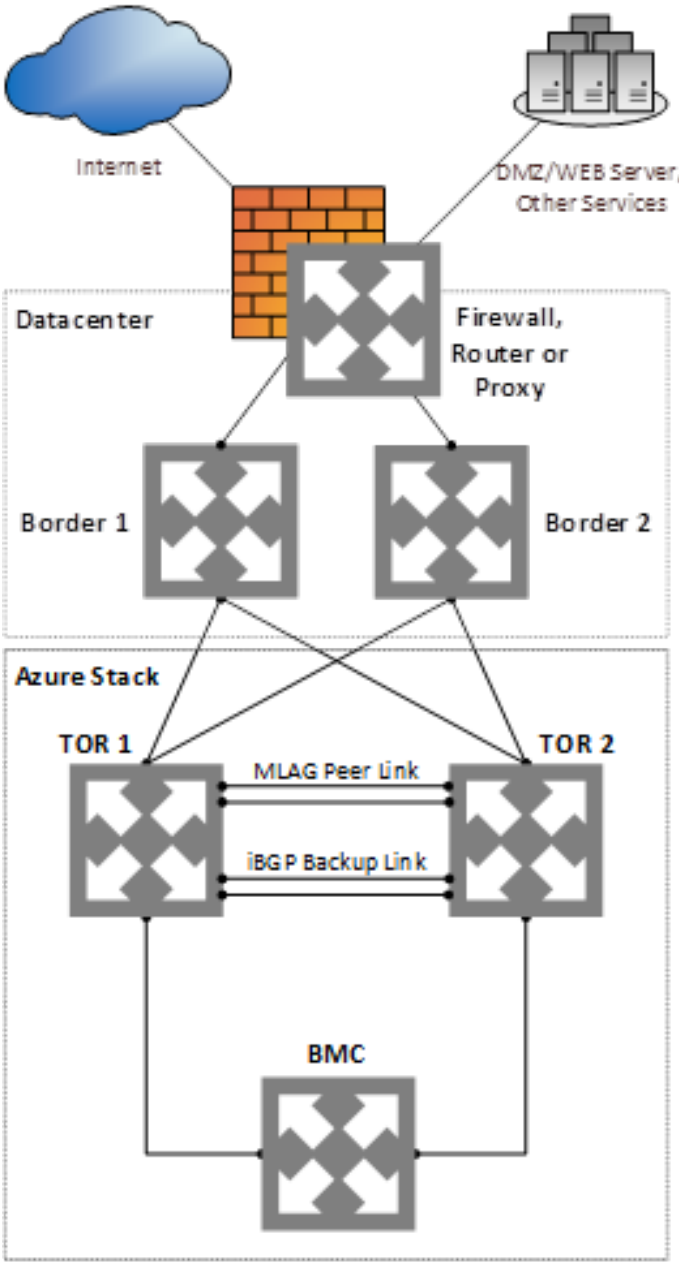

Figure 48. Proxy networking

For the latest Microsoft guidance about network integration and border connectivity, see Border connectivity on the Microsoft website.

Firewall integration

We recommend that you use a firewall device to help secure Microsoft Azure Stack Hub. Although firewalls can help with distributed denial-of-service (DDOS) attacks, intrusion detection, and content inspection, they can become a throughput bottleneck for Azure storage services, such as BLOBs, tables, and queues.

For information about how to plan for firewall integration, see Publish Azure Stack Hub services in your datacenter on the Microsoft website. The article lists the inbound and outbound ports and protocols that are required for Azure Stack Hub.

Deployment

Services

One of the primary design goals of Dell Technologies is to enable customers to be operational in days rather than weeks. Achieving this goal requires substantial engineering rigor before the customer receives the system. Keeping deployments predictable and costs low ensures that the least amount of time is spent on site. Customers are ensured a smooth transition to get started building plans and onboarding tenants.

The Dell Technologies engineering labs put Microsoft software and Dell Technologies hardware, software, and firmware through a suite of functional, performance, and reliability tests with a focus on standardizing and automating as much as possible. The team at the Dell Technologies factory runs additional pre-deployment tests to ensure that every system is not only fully integrated but that all possible issues are eliminated before shipping to the customer.

After the rack is in place, Dell Technologies technical engineers configure and integrate the hybrid-cloud environment, resulting in a fully operational platform that is ready—within days—to deliver services with Microsoft Azure Stack Hub.

The following table describes the Dell Technologies deployment services for the solution.

Table 37. Deployment services

Attributes	Details
Service type	Fixed Price/Fixed Scope Service
Support and Deployment Services (SDS)	On-site hardware configuration and implementation of Dell Integrated System for Microsoft Azure Stack Hub
Consulting Services	Remote implementation of Microsoft Azure Stack Hub Customer handoff includes: What to do next Where to go for more information Whom to contact for support

Registering Azure Stack Hub

Registering Microsoft Azure Stack Hub with Azure enables you to download marketplace items from Azure and to set up commerce data reporting back to Microsoft

For more information, see Register Azure Stack Hub with Azure on the Microsoft website.

NOTE: German and U.S. government cloud subscriptions are not currently supported.

6

Operations and Management Software

Topics:

- Microsoft azure stack hub software
- Hardware lifecycle host software

Microsoft azure stack hub software

Microsoft Azure Stack Hub

Microsoft Azure Stack Hub is an extension of Azure, bringing cloud computing to on-premises environments.

For more information, see Azure Stack Hub overview on the Microsoft website.

Accessing Azure Stack Hub

There are two portals in Microsoft Azure Stack Hub: Administration and User (also referred to as the Tenant portal). The following table provides sample URLs to access Azure Stack Hub.

Table 38. Portals

Portal	URL
Administration	adminportal.<region>.<fqdn>
User	portal.<region>.<fqdn>

Administration portal

The Administration portal, as shown in the following figure, enables a cloud operator to perform administrative and operational tasks.

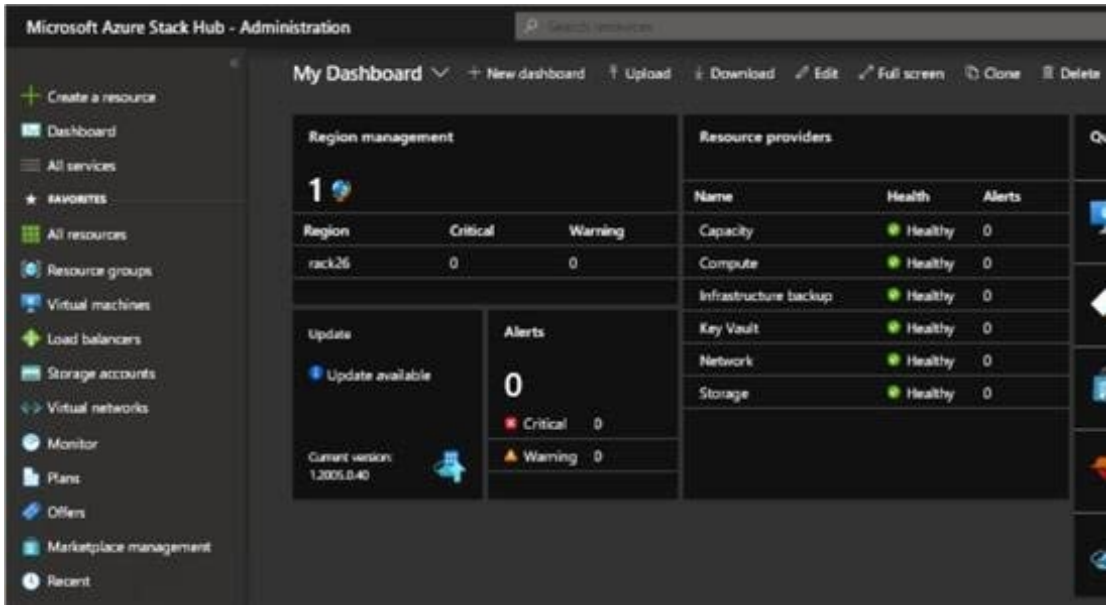

Figure 49. Microsoft Azure Stack Hub Administration portal – Dashboard view

A cloud operator can:

- Monitor health and alerts
- Manage capacity
- Populate the marketplace
- Create plans and offers
- Create subscriptions for tenants

A cloud operator can also create resources such as VMs, virtual networks, and storage accounts.

User portal

The user portal does not provide access to any of the administrative or operational capabilities of the administration portal. In the user portal, a user can subscribe to public offers, and use the services that are made available through those offers.

Privileged Endpoint

Privileged Endpoint (PEP) is a PowerShell Just Enough Access (JEA) endpoint. The PEP is accessed through the Dell Technologies alerting and monitoring system VMs.

There is no access to Microsoft Management Console (MMC) snap-ins, Azure Service Fabric Explorer, and so on. Unlocking the PEP is known as “breaking the glass”, and only Microsoft or Dell Technologies support can unlock the PEP.

Hardware lifecycle host software

Microsoft Windows Server 2019 Datacenter edition

Windows Server 2019 is the cloud-ready operating system that supports the current workloads while introducing technologies that make it easy to transition to cloud computing when you are ready. Dell Technologies HLH uses Windows Server 2019 Datacenter edition with Hyper-V to host the Dell Technologies management VMs and the patch and update tools.

Dell Technologies Secure Connect Gateway (SCG)

SCG is an application that automates technical support for your Dell server, storage, and networking devices. SCG monitors your Dell devices and proactively detects hardware issues that may occur. When a hardware issue is detected, SCG automatically opens a support case with Technical Support and sends you an email notification.

7

Security

Topics:

- Security overview
- Least-privilege authority
- Secrets rotation

Security overview

Security that is incorporated into the design is a key tenet of Microsoft Azure Stack Hub. Security features enabled for the solution include:

- **Firmware**
  - TPM 2.0 and SecureBoot are enabled.
  - All firmware and driver update packages are signed.
  - The firmware update is secured and uses Windows Cryptograms implementations.
- **Software**
  - BitLocker is enabled on all hard drives.
  - Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG) class security policies are applied and enabled.
  - Device guard and credential guard are enabled.
  - Allowlisting is enabled to ensure that unknown software cannot be run on host systems.
  - Defender is enabled on the HLH host for anti-malware.
  - Federal Information Processing Standards (FIPS) 140-2 compliant crypto algorithms are used for internal stack communication.
- **Network traffic**
  - The network is encrypted.

Least-privilege authority

Dell Technologies hardware and software can enable multiple roles and users. To ensure security and meet least-privilege authority requirements for Azure Stack Hub, Dell Technologies defines the operator and administrator roles at deployment to designate the minimum authority that is required to perform each operation:

- **Operator**—Minimum privilege to read but not modify
- **Server Admin**—Full access to update, modify reboot, and so on
- **Switch Admin**—Full access to reboot and update

Dell Technologies deployment engineers can help customers enable additional users and roles for the HLH.

NOTE: Microsoft defines and controls Azure Stack Hub roles, which cannot be changed.

Secrets rotation

Overview

We recommend, on a regular cadence, that you rotate secrets that are contained in the switches, HLH, and iDRACs, for example, passwords, certificates, or string keys. At the end of the deployment period, Dell Technologies assists the operator, if required, to set up accounts and remove any well-known user names and passwords.

For more information about guidance on secrets in use and how to use the available tools, see Rotate secrets in Azure Stack Hub on the Microsoft website.

The following table lists the supported Azure Stack Hub rotation matrix.

Table 39. Microsoft Azure Stack Hub supported rotation

Certificate installed	Rotate certificate to	Supported	Azure Stack Hub release
Self-Signed	Enterprise	Not supported	N/A
Self-Signed	Public	Supported	1803 and later
Self-Signed	Self-Signed	Not supported	N/A
Enterprise	Public	Supported	1803 and later
Enterprise	Self-Signed	Not supported	N/A
Enterprise	Enterprise	This is supported in 1803 if customers use the same enterprise CA that is used at deployment	1803 and later
Public	Self-Signed	Not supported	N/A
Public	Enterprise	Not Supported	N/A
Public	Public	Supported	1803 and later

NOTE: We do not recommend using well-known user names such as ADMIN, admin, root, Administrator, USERID, and so on, or weak passwords, such as Password, Password1!, P@ssW0rd, Welcome, 1234567, Winter10, Calvin, and so on.

HLH-related password changes

By default, Windows Server 2019 account passwords on the HLH host and Management VM are set to expire after 30 days. This default includes the Administrator accounts and any other operator accounts that are created during deployment. These operating system account passwords can be changed through the system settings in Windows Server 2019.

If the passwords are allowed to expire, then you must open a console session to perform a reset; RDP connections are unable to connect if the password has expired. For the Management VM, you can open the console session from the Hyper-V manager on the HLH host. For the HLH host, you must use a physical console or iDRAC virtual console.

NOTE: We recommend that you create strong passwords that include at least one each of uppercase and lowercase letters, numerals, and special characters.

8

Maintaining the Solution

Topics:

- Monitoring and alerting in Azure Stack Hub
- Patch and update
- Node expansion

Monitoring and alerting in Azure Stack Hub

The Health resource provider monitors health and generates alerts for each component to the Microsoft Azure Stack Hub Administration dashboard from:

- Internal Health Services
- System Health Tests

For more information about Azure Stack Hub health and alerts monitoring, see Monitor health and alerts in Azure Stack Hub on the Microsoft website.

Patch and update

One of the key challenges that system operators face is to safely and reliably update their Azure Stack Hub infrastructure while providing highly available, mission-critical services to customers. Updates can range in scope from software to hardware across the core components of the system. Microsoft and Dell Technologies provide customers with the ability to update their infrastructure while ensuring that business applications, services, and workloads are highly available.

To ensure that updates are completed smoothly and efficiently, Dell Technologies provides tools that are on the HLH to update Dell Technologies software and firmware.

To simplify the Azure Stack Hub update process, Microsoft provides an **Update Resource Provider** and **Updates** functions in the **Administration** portal native to a multinode Azure Stack Hub deployment. The **Updates** function enables you to:

- View important information such as the current stamp version.
- Install updates.
- Review update history for previously installed updates.

As an operator installs updates, they can view the high-level status as the update process iterates through various subsystems in Azure Stack Hub. Subsystems can include physical hosts, service fabric, infrastructure VMs, and services that provide both the administration and user portals.

Microsoft and Dell Technologies release update packages contain both a security- and non-security-related payload. Customers must keep their stamps current to maintain both security and functional environments.

NOTE: Maintenance operations can affect tenant workloads. We recommend that you notify users of the maintenance operation and that you schedule normal maintenance windows during nonbusiness hours as much as possible during the entire update process.

The current Dell Technologies update information is available under Integrated System for Microsoft Azure Stack Hub on the Online Support website.

The current Azure Stack Hub update information is available at Manage updates in Azure Stack Hub on the Microsoft website.

The patch and update process is a two-phase process:

1. Run the Dell Patch and Update Automation tool.
2. Run the Microsoft patch and update framework.

Firmware patches and updates are installed first before running software patches and updates. For the correct order, or for any additional instructions for both the Microsoft and the Dell updates, see the *Dell Integrated System for Microsoft Azure Stack Hub Patch And Update Installation Guide*.

A key tenet of Azure Stack Hub is to maintain consistency with Azure cloud. To ensure this consistency, Microsoft and Dell Technologies recommend that operators keep Azure Stack Hub up-to-date with the latest updates. The stack must not be more than three months behind on updates to ensure timely support.

For more information about the Microsoft servicing policy, see Azure Stack Hub servicing policy on the Microsoft website.

NOTE: The Dell Patch and Update Automation tool is an end-to-end automated process for patching and updating the HLH. The process caters to an automated update of firmware, drivers, and operating system updates for the HLH. SU node firmware is updated through the Azure Stack Hub Administration Portal.

Node expansion

Overview

Dell Technologies node expansion focuses on increasing the capacity of an existing solution that is powered by a Dell Integrated System (hybrid or all-flash scale unit). Node expansion offers flexibility to existing customers to increase their capacity in homogenous increments of either a single node, multiple single nodes, a set of four nodes, or multiple sets of four nodes. Each new scale unit node must be homogenous with the nodes present in the existing stack, which means that it has the same CPU type, memory, disk number, and disk size. Customers can expand their capacity up to 16 scale unit nodes.

Node expansion for the solution is an automated process. Full details are available in the *Dell Integrated System for Microsoft Azure Stack Hub Customer Node Expansion Guide*.

Node expansion workflow

The following figure shows the workflow of customer delivery and deployment of node expansion for the Dell Integrated System.

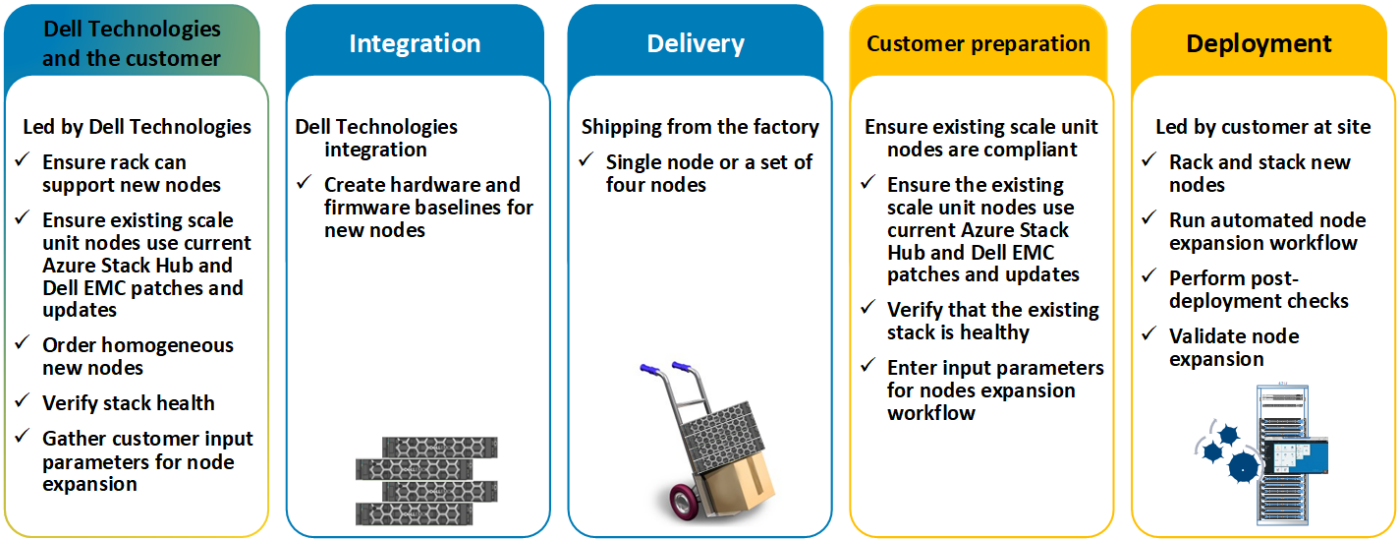

Figure 50. Customer delivery and deployment workflow for node expansion

The following figure shows the high-level workflow for adding an SU node to an Azure Stack Hub SU.

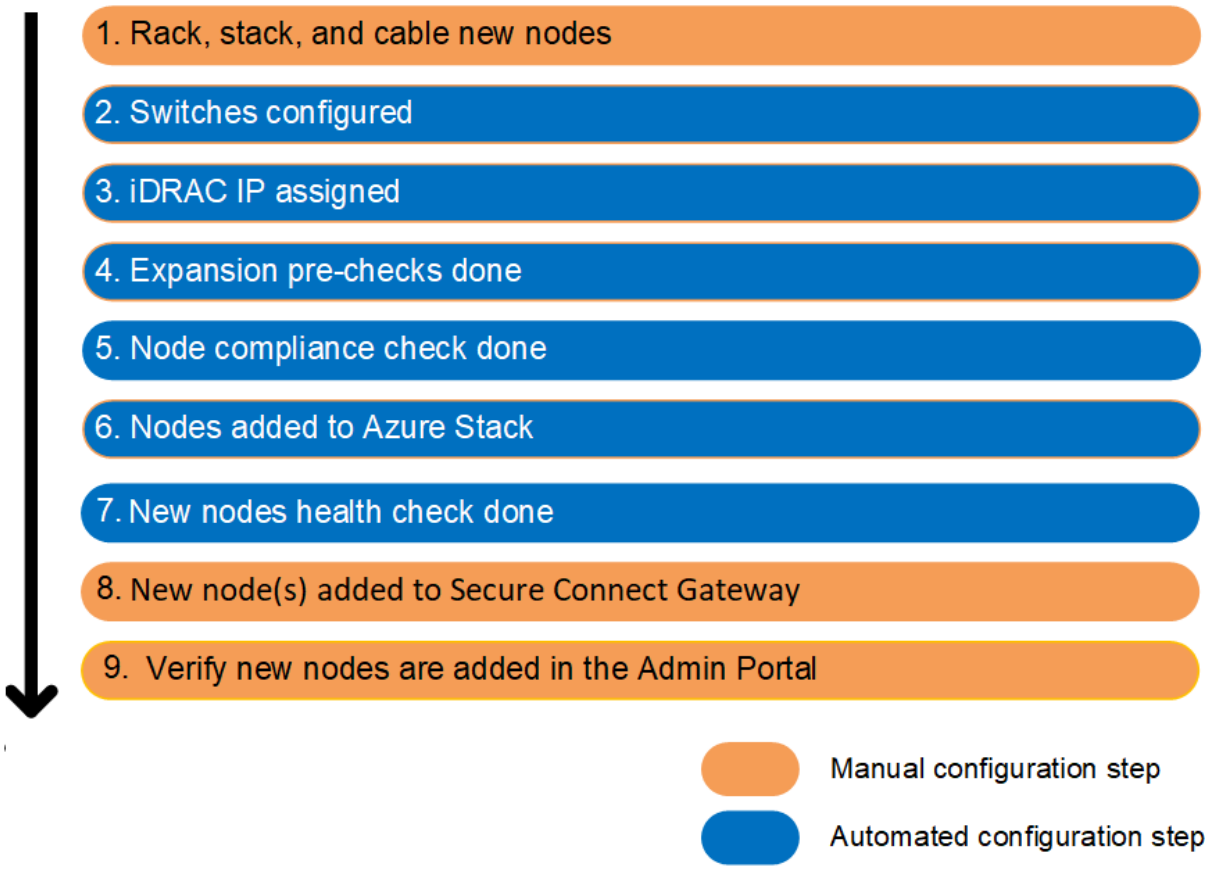

Figure 51. Node expansion workflow

Hardware components for node expansion

The following table lists the minimum hardware components that are required for the node expansion process.

Table 40. Hardware components for node expansion

Components	Quantity	Details
Operational Dell Integrated System for Microsoft Azure Stack Hub	1	Existing customers owning a Dell Integrated System server (hybrid, all-flash, or dense configuration) For details about the servers, see: PowerEdge R640 server for HLH and all-flash scale unit PowerEdge R740xd server for hybrid scale unit PowerEdge R840 server for dense and GPU scale unit
Additional scale unit nodes	1 or 4 (multiples)	You can only order scale unit nodes in quantities of one or four. All nodes in the integrated system must be homogenous, including the nodes that are being added. The total nodes (after the expansion is complete) cannot exceed sixteen.

Node expansion prerequisites

Node expansion requires a working Dell Integrated System to which new scale unit node or nodes are added. After they order new nodes, customers must ensure that the following prerequisites are met before installation:

- If new nodes are added to a customer rack, the rack (including the PDU) must be able to accommodate the new nodes.
- The existing Dell Technologies nodes must be up-to-date with the most recent versions of the Microsoft Azure Stack Hub and Dell patches and updates.
- The existing Dell Technologies server must be in a healthy state.
- The existing Dell Technologies server credentials and input parameters are required for the node expansion.

The Dell Technologies Support team can help customers with any queries.

Networking modification

Customers must modify their existing Dell Integrated System switch-ports configuration (ToRs and BMC) when adding new scale unit nodes as part of the Dell Technologies node expansion.

Deployment services

The following table lists the deployment services available to customers for a node expansion.

Table 41. Deployment services

Attributes	Description
Service type	Fixed Price/Fixed Scope Service
Support and Deployment Services (SDS)	On-site configuration and implementation of node expansion in the customer's existing solution Customer handoff includes: What to do next Where to go for more information Whom to contact for support

9

Backup and Recovery

Topics:

- Backup and recovery overview
- Tenant data backups
- In-scope data backups
- Microsoft PaaS resource providers
- Web application BCDR strategy
- HLH deployment collateral backup
- SMB target folder structure
- Recovery from a catastrophic failure

Backup and recovery overview

This chapter provides business continuity and disaster recovery (BCDR) recommendations to help a cloud operator effect a full recovery of Microsoft Azure Stack Hub infrastructure components from a catastrophic event, requiring a redeployment of Microsoft Azure Stack Hub on hardware.

This guide is intended to complement the Microsoft-provided recovery procedures for Azure Stack Hub for Dell Technologies customer deployments.

NOTE: This guide does not cover procedures that are required to recover in-guest or tenant data.

Backup requirements

You can enable a backup when you are ready to put your cloud into production. Do not enable backup if you plan to do testing and validation for a long time.

Before you enable the backup service, ensure that you have all the backup requirements in place.

For more information, see What is the Azure Backup service? on the Microsoft website.

Tenant data backups

Azure Stack Hub separates infrastructure data from tenant data. This guide describes only the infrastructure aspects of data recovery.

Tenants of Azure Stack Hub are responsible for protecting their workloads and backing up data in the event of the following scenarios:

- Recovery of the Azure Stack Hub stamp is impacted by a catastrophic data loss
- Recovery of individual services is impacted by data loss

In-scope data backups

Azure Stack Hub Infrastructure Backup Service protects the following data:

- Deployment inputs
- Internal identity systems
- Federated identify configuration (disconnected deployments)
- Root certificates used by internal certificate authority

- Azure Resource Manager configuration user data, such as subscriptions, plans, offers, and quotas for storage, network, and compute resources
- KeyVault secrets and vaults
- RBAC policy assignments and role assignments

None of the user IaaS or PaaS resources are recovered during deployment, which means that IaaS VMs, storage accounts, BLOBs, tables, network configuration, and so on, are lost.

The purpose of cloud recovery is to ensure that your operators and users can log in to the portal after deployment is complete. Users logging in will not see any of their resources. Users have their subscriptions and the original plans and offers policies, which the administrator defines, restored. Users logging in to the system operate under the same constraints that the original solution imposed before the disaster. After cloud recovery is completed, the operator can manually restore value-add and third-party resource providers and associated data.

Microsoft PaaS resource providers

Microsoft offers the following resource providers:

- Microsoft SQL Server, see Deploy the SQL Server resource provider on Azure Stack Hub
- MySQL, see Deploy the MySQL resource provider on Azure Stack Hub
- App Service, see Deploy App Service in Azure Stack Hub

Web application BCDR strategy

Protecting cloud-born applications requires a deeper discussion and a clearer understanding of the top-down BCDR strategy for applications. A “bottom-up” strategy, where the underlying physical hypervisor is the source, does not work, especially for PaaS-based applications.

You must understand how tenants are protecting their cloud-born applications in Azure (or AWS, GCS, and so on). In all cases, the services do not expose an infrastructure backup that targets the underlying computers running complex multitenant services.

Backup is delegated up the stack to the application/tenant. For example, most services expose create, read, update, and delete (CRUD) operations. Administration, development, and development operations can use the services to protect a specific resource, such as backup of an application service or database, replication of a BLOB, and so on.

No single operation backs up all data repositories across all applications and subscriptions. This approach has limitations if you want an application-consistent backup across multiple independent data repositories. There is no virtual switching system (VSS) for PaaS. Over the long term, the most sophisticated application provides native backup and restore capabilities that account for consistency, item level restore, failover, and so on.

As Microsoft ships new PaaS offerings, it offers a consistent set of capabilities for Azure Stack Hub. Each service cannot provide all capabilities on Day One, but Microsoft will close any gaps over time. Microsoft documents the backup and restore workflows that work for each service. For example, Microsoft does not currently support read-access geo-redundant storage (RA-GRS) for BLOB storage. This limitation affects how you design BCDR for an application. You can take a snapshot of a BLOB and copy it to another storage account, but the native replication of BLOBs between two regions is not yet available.

Third-party solutions

Because modern web applications use standard CRUD operations, viable third-party solutions exist to address continuity.

A solution such as ZeroDown ZeroNines can fill the niche for synchronizing data inbound to a web application by journaling the CRUD operation and playing back across multiple cloud targets. This decoupling of the inbound URI/CRUD command is a newer approach to addressing BCDR for web applications.

For more information, see ZeroDown Software.

Custom images and BLOB collateral for the marketplace

Due to the finite focus of the Infrastructure Backup Service, you must consider the infrastructure aspects that custom VM images represent, which are stored as BLOBs in the Azure Stack Hub cloud.

Protect your custom images and marketplace packages in addition to your other valuable data, and account for their recovery and re-creation in the event of a site recovery.

HLH deployment collateral backup

We recommend that you use the SMB share or NAS targets to store the collateral you used to deploy the Azure Stack Hub, and the switch-configuration backup information.

During the HLH and Azure Stack Hub deployment, the deployment engineer copies important configuration files, such as switch configurations, BitLocker recovery key, and deployment files, to a folder on the HLH. At the end of the deployment, the deployment engineer provides these files for backup along with any other backups.

SMB target folder structure

Infrastructure Backup Service creates a MASBackup folder automatically. This folder is a Microsoft-managed share. Azure Stack Hub stores its backup data in the MASBackup folder.

For more information, see Azure Stack Hub datacenter DNS integration.

Recovery from a catastrophic failure

If there is a catastrophic data loss but the hardware is still usable, you must redeploy Microsoft Azure Stack Hub. During redeployment, you can specify the storage location and credentials that are required to access backups. In this mode, there is no need to specify the services that need to be restored. Infrastructure Backup Service injects control-plane state as part of the deployment workflow.

If there is a disaster that renders the hardware unusable, redeployment is only possible on new hardware. Redeployment can take several weeks while replacement hardware is ordered and arrives in the data center. Restoring control-plane data is possible at any time. However, restoration is not supported if the version of the redeployed instance is more than one version later than the version used in the last backup.

The following figure shows the high-level workflow for the backup and restore process after a catastrophic failure.

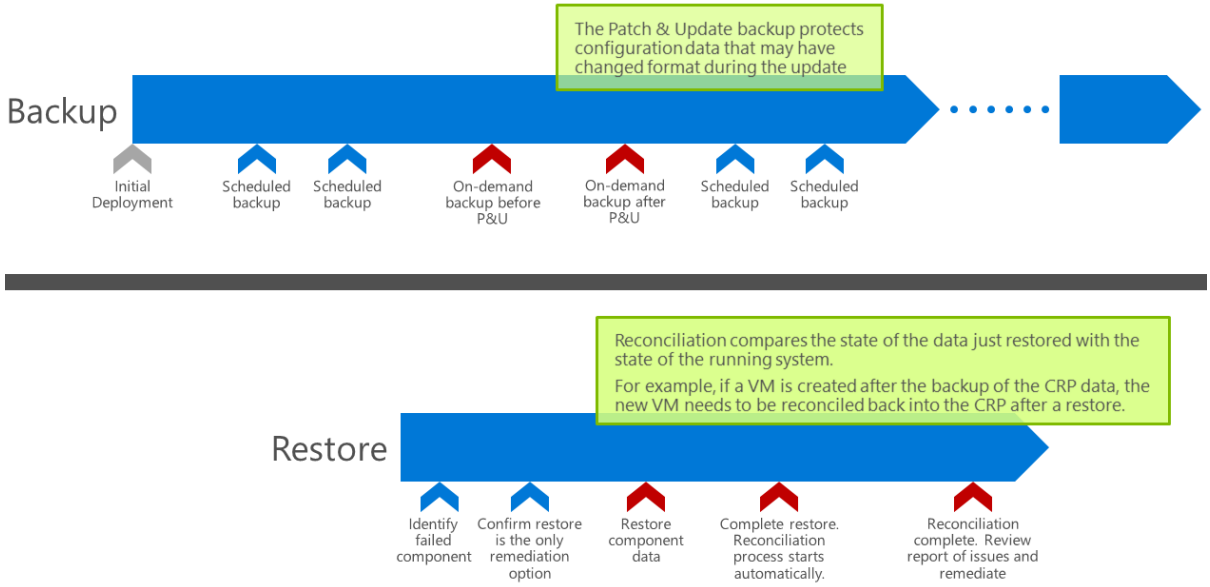

Figure 52. Recovery workflow

10

Conclusion

Topics:

- Summary

Summary

Dell Integrated System for Microsoft Azure Stack Hub is a cloud platform that provides Azure services and enables connectivity to the Azure public cloud. Dell Integrated System offers IaaS for rapid provisioning of VM-based workloads. It also enables you to provide Microsoft SQL, MySQL, and other PaaS offerings to your organization.

Dell Integrated System is engineered with Dell Technologies servers, networking, backup, and encryption, along with Microsoft application-development tools. Dell Technologies manages the component lifecycle of the entire Dell Integrated System platform to ensure that all phases are repeatable and predictable.

A

License Retrieval

This appendix presents the following topics:

Topics:

- Retrieving Dell Technologies licenses
- iDRAC license

Retrieving Dell Technologies licenses

This section describes how customers can locate their licenses in Software Licensing Central and Dell Digital Locker.

NOTE: During deployment planning, the Dell Technologies Deployment Project Manager can guide the customer through the license retrieval process, if necessary. The license must be available before starting the Dell Integrated System deployment.

Table 42. Dell Integrated System - HLH license management mechanisms

Product generation	iDRAC license management mechanism	
Dell Integrated System for Microsoft Azure Stack Hub on 14G servers Examples: PowerEdge R740xd, PowerEdge R640	Dell Digital Locker	

iDRAC license

Dell Digital Locker is an online repository where you can store and manage Dell Technologies software license keys. When you purchase a license, Dell Technologies sends an email with instructions to create a Dell Digital Locker account. Log in to your account at Dell Digital Locker to manage your license.

Dell Integrated System for Microsoft Azure Stack Hub comes with the following license:

- **iDRAC**: Dell Technologies embeds the iDRAC Enterprise Edition license in all your Dell Integrated System servers.

Retrieving your iDRAC licenses

Prerequisites

To retrieve a license:

Steps

1. Go to Dell Digital Locker and click **Sign In**.
2. Sign in to your **Dell My Account** using the email address that was used at the time of purchase or that was used to assign your software licenses.

   For questions about creating or updating a Dell Digital Locker account, see Dell Order Support FAQs.

   If you cannot find your purchase order email or log in to your Dell Digital Locker, contact your sales team, find your order number, or request order support online.

B

Dell Technologies Support and Consulting Offerings

This appendix presents the following topics:

Topics:

- Azure Stack Hub implementation requirements
- Field replacement of parts
- ProSupport Plus for Enterprise
- Consulting service offerings
- Additional resources

Azure Stack Hub implementation requirements

Customers cannot install the Dell Integrated System hardware for the solution. Dell Technologies resources or a certified deployment partner must perform the hardware rack deployment, hardware configuration, and Azure software implementation services.

Custom scope offering

The following figure shows the required steps to customize Microsoft Azure Stack Hub for your environment.

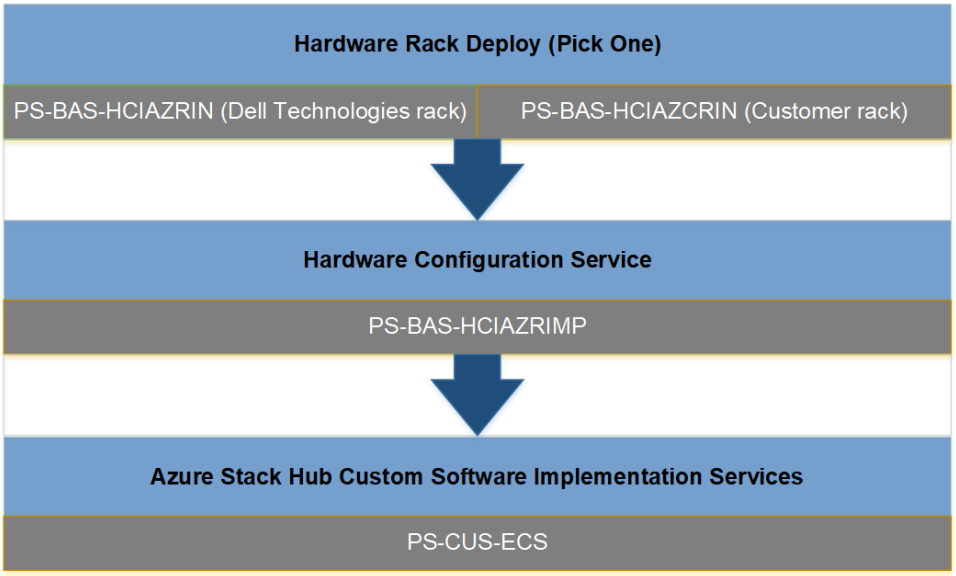

Figure 53. Custom scope offering

Fixed price/fixed scope offering

The following figure shows the required steps for a standard Microsoft Azure Stack Hub deployment.

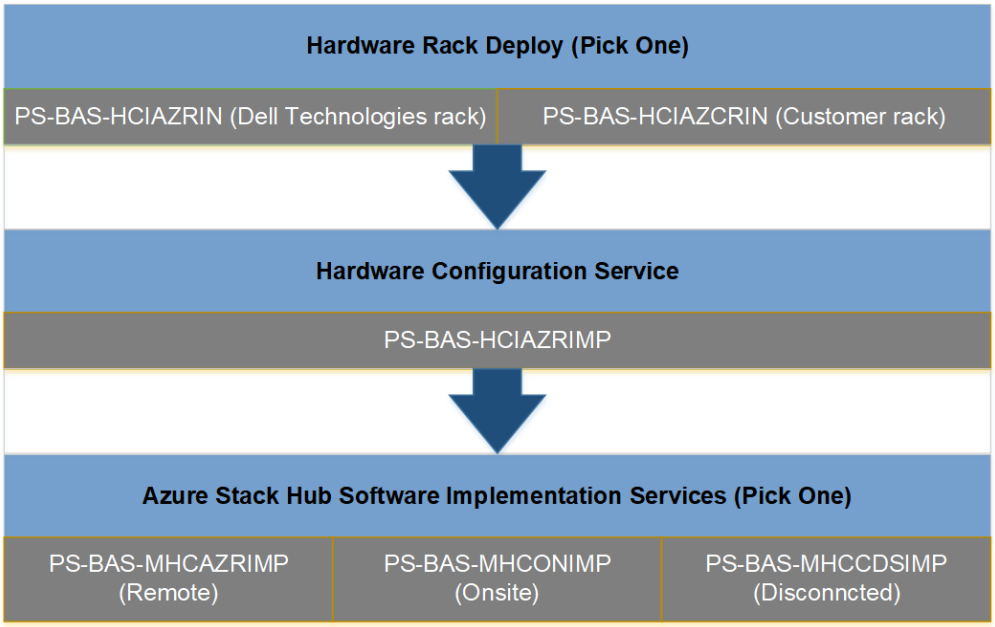

Figure 54. Fixed price/fixed scope offering

NOTE: With the Disconnected-from-Azure deployment option, you can deploy and use Microsoft Azure Stack Hub without a connection to the Internet. However, with a disconnected deployment, you are limited to an ADFS identity store and the capacity-based billing model.

Field replacement of parts

If a part fails while in the customer's data center, the customer is not responsible for resolving the problem. Dell Technologies owns the replacement process and will fix the broken part and bring the system back to its functioning state.

Also, SLAs prevent troubleshooting beyond a few times. After a reasonable number of attempts, Dell Technologies will replace the entire node. Due to the pre-deployment testing process, the solution has integrated automation that provides alerts of any failures to enable rapid replacement for minimal disruption.

ProSupport Plus for Enterprise

The following figure provides a comparison of the ProSupport and ProSupport Plus services.

Table 43. ProSupport services comparison

Service	ProSupport	ProSupport Plus
Remote technical support	24x7	24x7
Onsite support	Next Business Day or Mission Critical	Mission Critical
Automated issue detection and case creation	Yes	Yes
Self-service case initiation and management	Yes	Yes
Hypervisor, operating environment software, and operating system support	Yes	Yes
Priority access to specialized support experts		Yes

Table 43. ProSupport services comparison (continued)

Designated service account management expert		Yes
Periodic assessments and recommendations		Yes
Monthly contract renewal and support history reporting		Yes
Systems maintenance guidance		Semi-annual

ProSupport Plus provides the following benefits:

- **Better system performance and health**—Dell Technologies experts and tools help you avoid problems that are associated with incompatible hardware, software, and BIOS and firmware versions.
- **Collaboration**—Dell Technologies and your Technology Service Manager work with you during the entire process, from data collection through delivery and perform the analysis for you.
- **Automation**—SupportAssist Enterprise and the Dell Technologies alerting and monitoring system provide proactive, automated issue detection, notification, case creation, and reporting that reduces the systems maintenance data-collection effort.

The solution includes standard next-business-day parts replacement, which can be updated to four-hour replacement in many service areas.

Consulting service offerings

Our services for Dell Integrated System help customers implement and integrate Microsoft Azure Stack Hub into their existing environments. This service helps you prepare for the Dell Integrated System deployment by understanding the best use of the cloud for your business and how to optimize your integration.

Accelerate your path to productivity with deployment and integration services:

- Using our experience and expertise with hybrid cloud platforms, we have engineered an optimal rack integration that ensures a consistent technology build, quality assurance, and comprehensive oversight from configuration to delivery.
- After the rack is in place, Dell Technologies technical engineers rapidly configure and integrate your Dell Integrated System environment, resulting in a fully operational platform that is ready to deliver services with Azure Stack Hub.

Many customers want to expand their hybrid-cloud solution to deliver more value to their business. Dell Technologies Services offer optional custom services to optimize Dell Integrated System:

- Extend your on-premises Active Directory with Azure Active Directory Federation providing a cloud-ready directory services platform with single sign-on.
- Consume and integrate with Microsoft Azure Stack Hub public cloud.
- Develop simple IaaS blueprints that are integrated into a service catalog to create complex anything-as-a-service (XaaS) offerings, such as database as a service (DBaaS) using SQL Server.
- For ongoing Day Two operations, take advantage of services to extend existing monitoring and metering systems by using Microsoft System Center.

When you purchase Dell Integrated System, you also receive single contact support with ProSupport Plus, which is the highest level of support available. ProSupport Plus gives IT teams the confidence that Dell Technologies experts fully support each component. Support includes a dedicated Technical Account Manager, 24-hour/7-day access to hardware and software engineers, and collaborative third-party assistance. These resources help to accelerate the time to value of your Dell Integrated System.

Additional resources

Tools for using Azure and Azure Stack Hub

To use Microsoft Azure Stack Hub tools, obtain an Azure Stack Hub compatible Azure PowerShell module. Unless you have installed from other sources, you can obtain the module from public package repositories through GitHub.

For more information, see:

- Download Azure Stack Hub tools from GitHub
- Azure/AzureStack-Tools on GitHub

Online documentation

For information about:

- Microsoft Azure Stack Hub, see Azure Stack Hub Operator Documentation