ARVO
TECNOLOGIA

PROPOSTA COMERCIAL

CLIENTE
CJF

PREGÃO ELETRÔNICO
15/2023

DATA
05/01/2024

VALIDADE
90 Dias

FORMULÁRIO DE PREÇOS

Proponente: Arvvo Tecnologia, Consultoria E Serviços Ltda
CNPJ: 25.359.140/0001-81
Inscrição Estadual: 07.778.347/001-93
Endereço: Shn Quadra 1 Bloco A Sala 1.114, Ed. Le Quartier, Asa Norte, Brasília-DF - 70.701-010
Email: contato@arvvo.com.br
Telefone: (61) 3553-9006
Representante Legal: André Luiz Alves De Oliveira
RG: 1.685.233
CPF: 705.590.401-30
Banco: Itaú – Agência: 3213 - CC: 97.466-4

1) Preço à vista com tributos, insumos e demais encargos da contratação.
2) Pagamento exclusivamente por ordem bancária.
3) Validade: 90 dias.

Lote Único										
Item	Descrição	Marca/Modelo	Unidade de Medida	CJF	TRF1	TRF2	TRF6	Total	Custo Unitário	Custo Total
1	Subscrição de licenças de software para proteção de dados para 60 meses	Veritas NetBackup 10.3	Front EndTerabyte	180	655	760	450	2045	R$ 22.400,00	R$ 45.808.000,00
2	Subscrição de solução de backup para o Microsoft 365 por 60 meses	Veritas Alta SaaS Protection	Usuários	600	10560	6000	4000	21160	R$ 1.194,50	R$ 25.275.620,00
3	Appliance de backup para armazenamento de dados para curta retenção com garantia por 60 meses	Veritas Flex Appliance 5260	Equipamentos	1	15	3	1	20	R$ 400.000,00	R$ 8.000.000,00
4	Expansão do Appliance de backup para armazenamento de dados para curta retenção com garantia por 60 meses	Veritas Shelf Flex Appliance 5260	Expansão de Equipamentos	5	10	11	2	28	R$ 324.000,00	R$ 9.072.000,00
5	Appliance de backup para armazenamento de dados para longa retenção com garantia por 60 meses	Veritas Access Appliance 3350	Equipamentos	1	2	3	0	6	R$ 1.998.000,00	R$ 11.988.000,00
6	Expansão de Appliance de backup para armazenamento de dados para longa retenção com garantia por 60 meses	Veritas Shelf Access Appliance 3350	Expansão de Equipamentos	0	2	2	2	6	R$ 162.000,00	R$ 972.000,00
7	Serviço de Instalação e configuração	-	Serviço	1	14	3	1	19	R$ 25.000,00	R$ 475.000,00
8	Transferência de conhecimento	-	Turma	1	1	1	1	4	R$ 12.000,00	R$ 48.000,00
9	Suporte técnico especializado de toda a solução por 60 meses	-	Serviço	1	14	3	1	19	R$ 140.000,00	R$ 2.660.000,00
Total										R$ 104.298.620,00

O VALOR TOTAL DOS ITENS DA PROPOSTA DE PREÇOS É DE R$ 104.298.620,00 (cento e quatro milhões, duzentos e noventa e oito mil, seiscentos e vinte reais).

Declaramos conhecer e aceitar todas as condições estabelecidas no Edital e seus anexos, bem como nos esclarecimentos publicados pelo CJF para o edital.

Declaramos que o detalhamento dos itens seguirão em anexo próprio juntamente com as comprovações técnicas e datasheets.

Declaramos que no preço proposto, estão inclusos todos os custos necessários, bem como todos os tributos, encargos trabalhistas, comerciais, custos com infraestrutura e quaisquer outras despesas que incidam ou venham a incidir sobre o objeto, e que influenciem na formação dos preços desta Proposta.

Brasília – DF, 05 de janeiro de 2024.

ANDRE LUIZ ALVES DE OLIVEIRA:70559040130

Assinado de forma digital por ANDRE LUIZ ALVES DE OLIVEIRA:70559040130
Dados: 2024.01.05 14:24:22 -03'00'

ARVVO TECNOLOGIA, CONSULTORIA E SERVIÇOS LTDA

André Luiz Alves de Oliveira

Cargo: Sócio-Diretor

RG: 1.685.233 SSP/DF

CPF: 705.590.401-30

DECLARAÇÃO DO SUBITEM 6.11.1
DECLARAÇÃO DE NÃO CONDENAÇÃO JUDICIAL

Conselho da Justiça Federal

Pregão Eletrônico: **15/2023**

Declaro que eu, **André Luiz Alves de Oliveira**, portador do CPF nº 705.590.401-30, representante da empresa **ARVVO Tecnologia, Consultoria e Serviços LTDA**, inscrita no CNPJ/MF sob. nº. 25.359.140/0001-81, estabelecida no endereço SHN Quadra 1 Bloco A Sala 1.114, Ed. Le Quartier, Asa Norte, Brasília-DF, como seu representante legal para os fins da presente declaração, que nos 5 (cinco) anos anteriores à divulgação deste edital, esta empresa não foi condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista.

Brasília/DF, 28 de dezembro de 2023.

ANDRE LUIZ ALVES DE OLIVEIRA:70559040130

Assinado de forma digital por ANDRE LUIZ ALVES DE OLIVEIRA:70559040130
Dados: 2023.12.28 15:43:46 -03'00'

ARVVO TECNOLOGIA, CONSULTORIA E SERVIÇOS LTDA
ANDRÉ LUIZ ALVES DE OLIVEIRA
SÓCIO/DIRETOR
CPF: 705.590.401-30

COMPROVAÇÕES AOS CRITÉRIOS DE SUSTENTABILIDADE

Conselho da Justiça Federal
Pregão Eletrônico: **15/2023**

Prezados Senhores,

A Arvvo tecnologia, consultoria e serviços Ltda, inscrita no CNPJ/MF nº. 25.359.140/0001-81, por intermédio de seu representante legal o Sr. André Luiz Alves de Oliveira, portador(a) do Documento de Identidade nº 1685233 e do CPF nº 705.590.401-30, em atenção as comprovações aos critérios de sustentabilidade, apresentamos documentos anexos de título:

Veritas 5260 Appliance - Pag. 61-61
Veritas Access 3350 Appliance - Pág. 78
INMETRO - Certificados – Veritas
Veritas-Declaration-of-Compliance-with-EU-RoHS-Directive

Bem como link oficial do fabricante:

https://www.veritas.com/support/en_US/compliance

Brasília/DF, 29 de dezembro de 2023

ANDRE LUIZ ALVES DE OLIVEIRA:70559040130

Assinado de forma digital por ANDRE LUIZ ALVES DE OLIVEIRA:70559040130
Dados: 2023.12.29 14:27:29 -03'00'

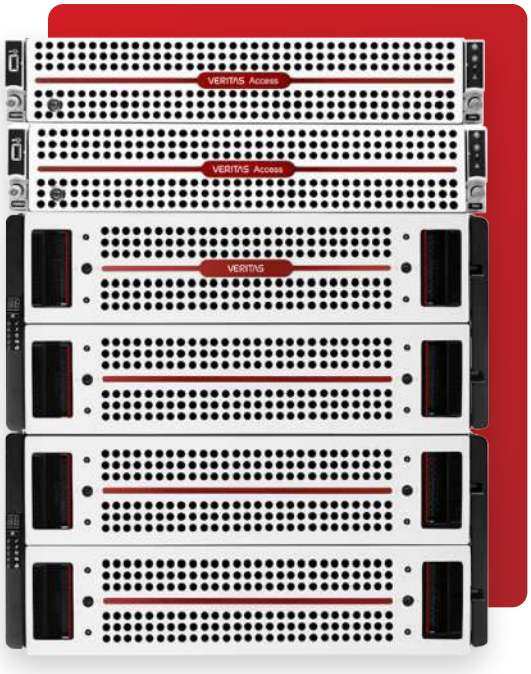
ARVVO TECNOLOGIA, CONSULTORIA E SERVIÇOS LTDA
ANDRÉ LUIZ ALVES DE OLIVEIRA
SÓCIO/DIRETOR
CPF: 705.590.401-30

NetBackup Access 3350 Appliance

Ransomware resilient long-term data retention with multi-cloud capability.

Overview

The NetBackup Access 3350 is a turnkey appliance designed to provide long-term retention in NetBackup environments. Deep integration with NetBackup means faster restores for LTR data sets and reduced overall storage costs with Global Dedupe. NetBackup's proven, enterprise-hardened deduplication saves space, improving storage efficiency and effective capacity by as much as 30x.



Access Appliance utilizes a multilayered security architecture that provides resilience against ransomware for the entire data protection infrastructure. At its core is immutable storage, an important component for ransomware resilience. Other layers include container isolation, a hardened operating system, access control and intrusion detection and prevention.

Automated tiering, via NetBackup Storage Lifecycle Policies, orchestrates data migration to on-premise and off-premise clouds to further reduce the operating cost, address additional capacity requirements, and increase the resilience of long-term data stores. Support for multiple protocols, including Amazon S3, CIFS/SMB and NFS, increases the utility of Access Appliance across the infrastructure where immutability and data tiering of unstructured data sets is required.

Like all NetBackup appliances, the Access 3350 comes with everything needed to put the system in production, including Access Software, which includes a pre-tuned operating system with security hardening, an integrated hardware platform that includes supportability enhancements and integration with NetInsights, Veritas' industry leading remote management application.

Access Appliance use cases include:

- **Cost-effective tape replacement**—Replace tape-based storage to meet demanding Recovery Time Objectives (RTOs) and reduce maintenance costs and additional software licensing required for many tape libraries
- **Archiving with Veritas Enterprise Vault™**—The Access 3350 works as a primary archive store, offering compliant and flexible storage for archive retention with remote replication capabilities
- **Hybrid Cloud LTR Solution**—NetBackup Access facilitates tiering data to popular cloud platforms.

Product Highlights

- **NetBackup integration**—Provides consistent end-to-end long-term data retention and protection, complete with classification and global deduplication features
- **Ransomware Resilient with immutable storage and Hardened security including:**
  - Security Technology Implementation Guides (STIG)
  - Federal Information Processing Standards (FIPS)140-2
- **Highly scalable**—The Access 3350 starts at 280 TB of usable capacity and scales to 2.8 PB
- **Hybrid Multi-cloud capabilities**—Policy-based tiering orchestrates automated data migration to on-premise, off-premise or multi-cloud object stores
- **Flexible**—Simultaneously access files and objects over multiple protocols, including NFS, CIFS/SMB and Object Storage
- **Reduced management costs**—A single pane of glass manages multiple instances, including integration with NetBackup and Enterprise Vault
- **Reduce CapEx**—Cost-optimized for Long Term Retention and tuned for high-capacity workloads
- **Resilient hardware architecture**—Clustered nodes with multiple data paths, redundant hot swap power supplies, redundant fan modules, and RAID groups with hot pluggable disks, deliver greater data protection and system availability

Technical Specifications	
NetBackup Access Appliance Node[2]	
1 Gb Ethernet ports (per node)	4 (2 used for internode communication)
25-10 Gb SFP Ethernet ports (per node, 10 Gb SFP populated)	4
Dimensions H x W x D (Inches) / (cm) / Rack Units (U)	3.5 x 19.0 x 31.25 / 8.9 x 48.3 x 79.4 / 2U
Max weight (lbs / kg)	51.28 / 23.26
Typical power consumption (watts)	300
Max power consumption (watts)	1200
AC voltage range (Volts) (compute node voltage is auto-ranging)	90 to 140 180 to 264
AC frequency range (Hz)	47 to 63
Typical ampere ratings (A)	2.75 (90 to 140V)
Number of server nodes	2

NetBackup Access Appliance Storage Shelf		
Drive Capacity	4 TB	10 TB
Max number of drives	82	82
Usable capacity[1]	280 TB (255 TiB)	700 TB (636 TiB)
Dimensions H x W x D (Inches) / (cm) / Rack Units (U)	8.75 x 19.0 x 36.75 / 22.2 x 48.3 x 93.4 / 5U	
Max weight with disk drives (lbs / kg)	317 / 144	
Typical power consumption (watts)	1047 / shelf	
AC voltage range (Volts)	200 to 240	
AC frequency range (Hz)	50 to 60	
Typical ampere ratings (A)	5.65 (200 to 240V)	

Expansion Options	
Primary System Capacity	Expansion Shelf Options
280 TB (255 TiB) (4 TB drive capacity)	(1) 280 TB (255 TiB) Expansion Shelf or (1) 700 TB (636 TiB) Expansion Shelf
700 TB (636 TiB) (10 TB drive capacity)	(1–3) 700 TB (636 TiB) Expansion Shelves or (1) 280 TB (255 TiB) Expansion Shelf

NetBackup Access Appliance Storage Shelf	NetBackup Access 3350 Node	StorageShelf
Operating temperature (oF)/(oC)	(50 to 95)/(10 to 35)	(41 to 95)/(5 to 35)
Storage temperature (oF)/(oC)	(-40 to 158)/(-40 to 70)	(-40 to 158)/(-40 to 70) (-40 to 158)/(-40 to 70)
Operating humidity	10 to 80%	10 to 80%
Operating altitude (ft)/(m)	(-100-9,842)/(-30.5- 3,000)	(-328-9,842)/(-1000-3,000)
Max noise (dBA)	82	82
Typical cooling (BTU/hr)	1024 BTU/hr	3,573
Max cooling (BTU/hr)	4094 BTU/hr	4,241

Warranty Coverage

One (1) year parts replacement and 90 days software.

Protocol Standards Followed

IPMI 2.0, SMBIOS 2.5, SAS 3.0, ACPI rev 3, IP RFC0791

Safety and EMC Standard Compliance

GB4943-2001, IEC 60950-1, UL 60950-1, FCC 47 CFR Part

15 Subpart A, EN 60950-1, EMC Directive 2004/108/ EC, EN

55024: 1998+A1+A2, LVD Directive 2006/95/EC

1. Terabyte = 1012 bytes; 1 Tebibyte = 240 bytes
2. Each node has 2 x 10 Gb Ethernet ports available as a base configuration.
3. Two server nodes in each configuration.

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1554 04/22

VERITAS

The NetBackup Flex Deployment Mode on the 5250 Appliance

Ransomware resilience for critical data.

The Veritas NetBackup™ Flex deployment mode running on a 5250 Appliance provides ransomware resilience and the capacity and performance to consolidate smaller NetBackup domains into a single appliance.

Based on container technology, the NetBackup Flex deployment mode extends NetBackup data protection with multi-tenant capabilities to reduce data center costs, improve management efficiency and protect against ransomware and security threats.

Solution Highlights

Ransomware Resiliency

The NetBackup Flex Deployment Mode Immutable Architecture is multilayered to provide security and resilience for the entire data protection infrastructure. At its core is immutable storage important for ransomware resilience. Other layers include container isolation, a hardened operating system, access control and intrusion detection and prevention.

- APIs and Automation
  Integration of APIs for external 3rd party management and monitoring for operational efficiency. Support for tools like Grafana to monitor performance of platform and instances on NetBackup Flex Deployment Mode.
- Optimized for departmental and data center workloads
  The NetBackup 5250 provides more granularity in expansion, starting at 10 TB and expandable up to 442 TB usable capacity, making it ideal for remote locations as well as enterprise data centers.
- Reduce costs with consolidation
  Consolidate small existing NetBackup deployments on a 5250 Appliance with the multi-tenant capabilities of the NetBackup Flex deployment mode. Reduce the number of server and storage devices requiring setup, management, maintenance, power cooling, cabling and floor space, significantly reducing data center costs.
- On-demand response to rapidly changing business environments
  Rapidly deploy infrastructure by configuring application instances into a complete data protection solution. Build systems to meet the specific information needs of a department or business unit.
- Fast and easy upgrades
  Minimize planned maintenance time by simply installing a NetBackup container with a new release.
- Proactive monitoring with NetInsights Console.
- Monitors key hardware components and notifies the administrator of fault events.

Performance

The NetBackup Flex 5250 delivers 28 TB/hour throughput based on server-side deduplication with a 98 percent deduplication rate.
The NetBackup Flex 5250 delivers 124 TB/hour throughput based on client-side deduplication with a 98 percent deduplication rate.

Technical Specification	NetBackup Flex 5250	Expansion Shelf
Usable storage capacity (TB/TiB)	10/9.1, 40/36.4	72/65.5 per shelf
Expansion shelves	N/A	Up to 6 shelves
Minimum system usable capacity (TB/TiB)	10/9.1	
Maximum system usable capacity (TB/TiB)	442/402	
1 Gb Ethernet ports	4	N/A
25–10 Gb Ethernet ports	Up to 6	N/A
16 Gb Fibre Channel ports	Up to 8	N/A
Dimensions H x W x D cm (inches)	8.9 x 48.26 x 76.9 (3.5x19x30.25)	S-Series 8.89 x 48.26 x 60.20 (3.5 x 19 x 23.7) D-Series 8.7 x 48.2 x 53.9 (3.4 x 18.9 x 21.2)
Maximum weight, with disk drives	24.1 kg (53 lbs.)	S-Series 28kg (62 lbs.) D-Series 24.2kg (53.35 lbs.)
Typical power consumption (watts)	240	225
Maximum power consumption (watts)	500	600
Operating temperature (°F/°C)	50–95/10–35	50–95/10–35
AC voltage range (volts)	100–127 200–240	100–127 200–240
AC frequency range (Hz)	50 to 60	50 to 60

Warranty Coverage

One (1) year parts replacement and 90 days software.

Management

Through the Appliance Management Server.

Protocol Standards Followed

IPMI 2.0, SMBIOS 2.5, SAS 3.0, ACPI rev 3, IP RFC0791, IPv6

Safety and EMC Compliance

GB4943-2001, IEC 60950-1, UL 60950-1, FCC 47 CFR Part 15 Subpart A, EN 60950-1, EMC Directive 2004/108/EC, EN 55024: 1998+A1+A2, LVD Directive 2006/95/EC

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1320 05/22

NetBackup™ Flex 5260 Appliance

Cyber-resilient data protection for department-level workloads.

The NetBackup Flex 5260 appliance is a turnkey cyber-resilient data protection solution that reduces data center costs with improved management efficiency and bullet proof cyber resiliency. As a complete data protection solution with more than 400 TB of storage, it can be quickly deployed to protect critical workloads across the enterprise.

Solution Highlights

Cyber resiliency against all attack vectors

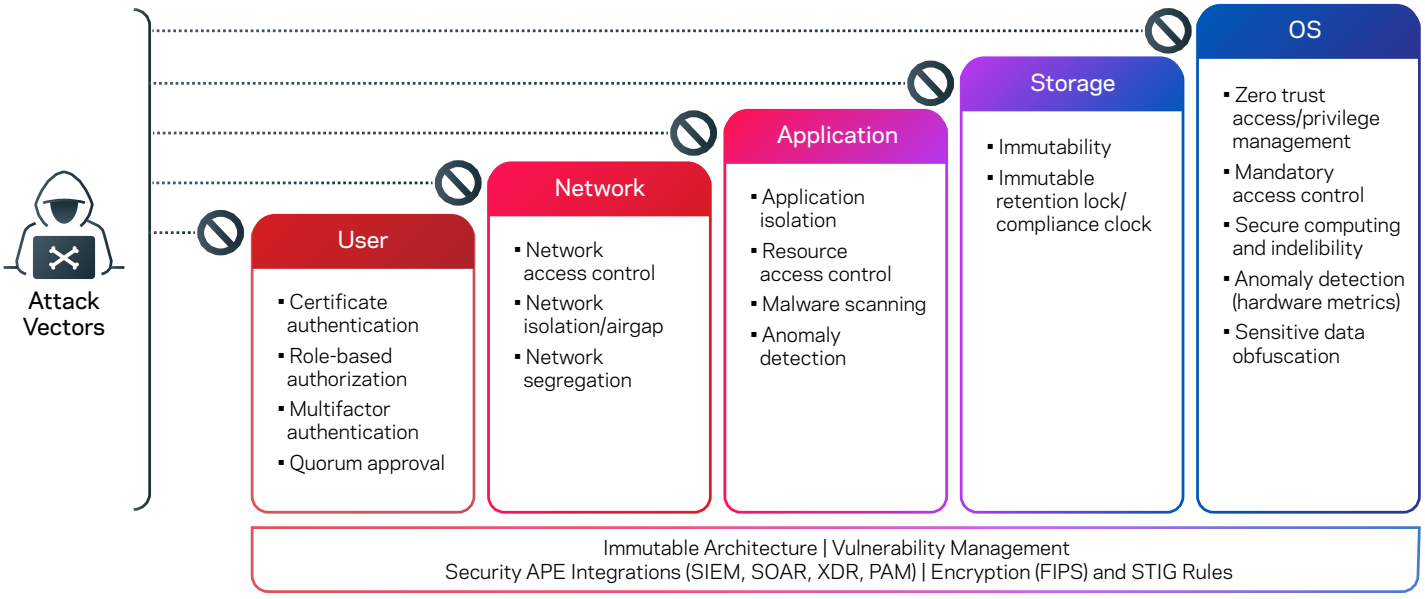


Figure 1. Veritas Appliances and Multi-Layered Security

Optimized for departmental and data center workloads

- Starting at 10 TB and expandable up to 442 TB usable capacity, the NetBackup Flex 5260 appliance provides the granularity to support remote locations, departments, and enterprise data centers

Proactive monitoring with NetInsights Console

- Monitors key hardware components, notifies the administrator of fault events, and makes recommendations for infrastructure optimization

Performance

The NetBackup Flex 5260 delivers up to 30.74 TB/hour throughput based on server-side deduplication, with a 98 percent deduplication rate.

Technical Specification	NetBackup Flex 5260	Expansion Shelf
Usable storage capacity (TB/TiB)	10/9.1, 40/36.4	72/65.5 per shelf
Expansion shelves	N/A	Up to 6 shelves
Minimum system usable capacity (TB/TiB)	10/9.1	
Maximum system usable capacity (TB/TiB)	442/402	
10Gb Ethernet (10GBASE-T)	4	N/A
25–10 Gb Ethernet ports	Up to 6	N/A
32 Gb Fibre Channel ports	Up to 8	N/A
Dimensions H x W x D cm (inches)	8.9 x 43.9 x 71.2 (3.5x17.28x28.03)	8.89 x 48.26 x 60.20 (3.5 x 19 x 23.7)
Maximum weight, with disk drives	25.46 kg (56.13 lbs.)	28kg (62 lbs.)
Typical power consumption (watts)	400	256
Maximum power consumption (watts)	1100	480
Operating temperature (°F/°C)	50–95/10–35	50–95/10–35
AC voltage range (volts)	90-140 180-264	100–127 200–240
AC frequency range (Hz)	50 to 60	50 to 60

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1918 07/23

Veritas NetBackup 10.3

Advanced data protection with integrated cyber resiliency.

Veritas NetBackup 10.3 builds on the existing foundations of NetBackup's secure by default architecture. The latest version expands intelligent, automated threat-detection support and integrates resiliency in recovery operations. The updates minimize attack surface and provide the most powerful and secure architecture to date. NetBackup continues to radically simplify data protection with the benefit of new resiliency features, advanced automation, and expanded workload support, all strengthening protection while reducing cost and resource demands.

Cyber Resiliency

More than 96% of business leaders identify ransomware as a critical threat and primary concern. Ransomware continues to grow: The number of attacks, amount of ransoms paid, and cost of related downtime are increasing exponentially. Securing your environment and data, as well as ensuring the ability to recover, are key requirements of any enterprise data protection strategy.

NetBackup's comprehensive data protection solution reduces risks, eliminates uncertainty, and helps you maintain control of your environment. The resiliency strategy reinforces your data and infrastructure defense against malicious data-damaging threats. Use it to confidently defend against ransomware for multi- and hybrid cloud using a three-step approach (Figure 1):

Step 1—Protect: Safeguard data integrity with system hardening, immutability, and air gap

Step 2—Detect: Monitor and report on system activity, leveraging AI/ML to mitigate threats and vulnerabilities

Step 3—Recover: Automate and orchestrate complete cross-system restoration with clean copies and non-disruptive

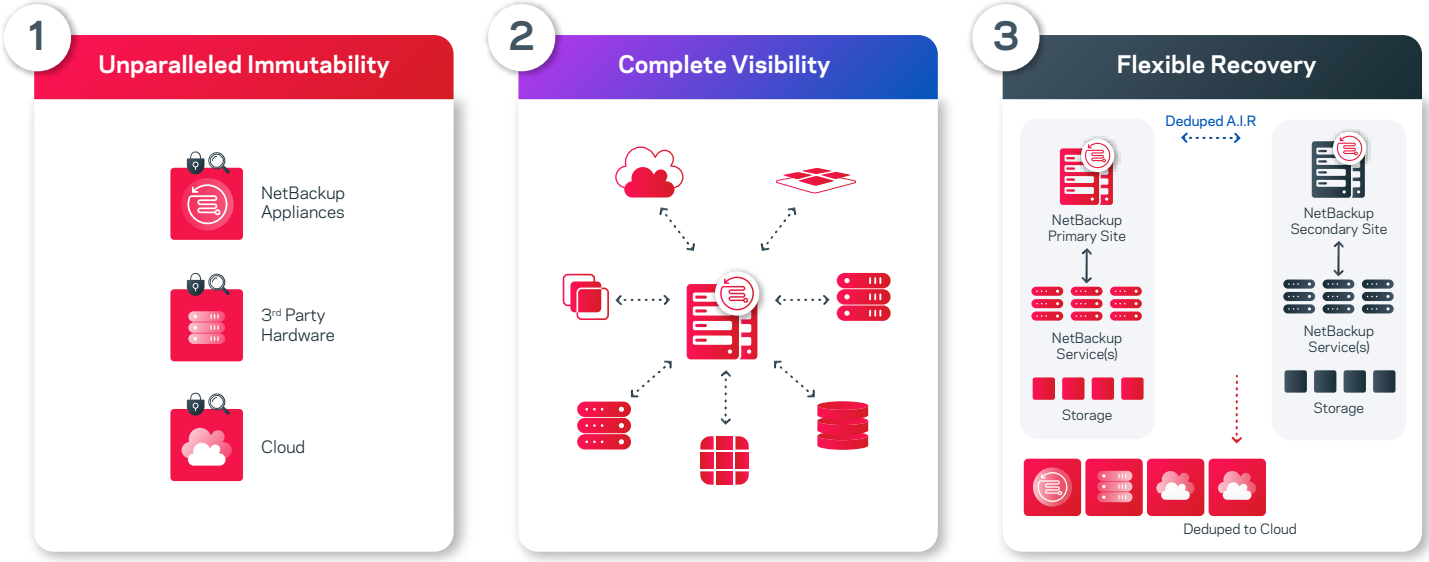


Figure 1. The three steps NetBackup takes to ensure cyber-resiliency

Enhancements for security, ransomware, and resiliency in Release 10.3 include:

- Multifactor authentication across all product interfaces, including GUI, CLI, and SSH
- Multi-person authorization for critical operations to prevent unauthorized data deletions and other malicious actions, along with a new internal tracking and ticketing system
- ML-based anomaly detection enhancements, which add user-behavior analysis and image-level entropy
- Integrated inline malware scanning during a restore including configurable options for handling of infected files
- FIPS compliance for Kubernetes workloads

AI-driven Anomaly Detection and Automated Malware Scanning

NetBackup augments its AI-driven anomaly detection capabilities with automated malware scanning. It checks for anomalies in near-real time during backup operations. If it suspects anomalies, it automatically initiates malware scanning of backups. In the case of a positive malware scan, it can automatically pause data protection, replication, and expiry of infected targets to contain the spread and prevent expiration of uninfected backups.

Release 10.3 leverages ML to further extend anomaly detection and audit trails to identify system-level or user behavior anomalies. It also adds the ability to analyze image-level entropy to aid the selection of recovery points using Veritas Alta™ View.

NetBackup 10.3 also uses malware scanning to identify the last-known good backup before restoring. Now early warning systems such as SIEM platforms can easily ingest anomaly and malware scan alerts stored within system logs. When combined with security alerts generated by other services, devices, and endpoints within the IT infrastructure, this data provides even greater visibility across an estate while increasing awareness and response to potential threats.

The enhancements allow NetBackup to pause data-protection activities including backups, duplication, and expiration automatically for the protected asset when a malware scan detects an infection in a backup image. The API also enables SOAR/XDR platforms to pause or resume these activities based on security or maintenance events.

Fast recovery of critical business operations relies on the ability to identify and recover the most recent malware-free backup. When recovering, it is also imperative to ensure any infected files are omitted. Excluding these files prevents the possibility of reinfection, enables recovery of the most current backups, and gets your business back to the closest point prior to the attack (Figure 2).

NetBackup 10.3 extends integrated malware scanning support with the ability to use inline malware scanning during recovery. This ensures a clean, automated recovery without additional steps from the user. And malware scanning support now includes cloud VMs and Universal Shares.

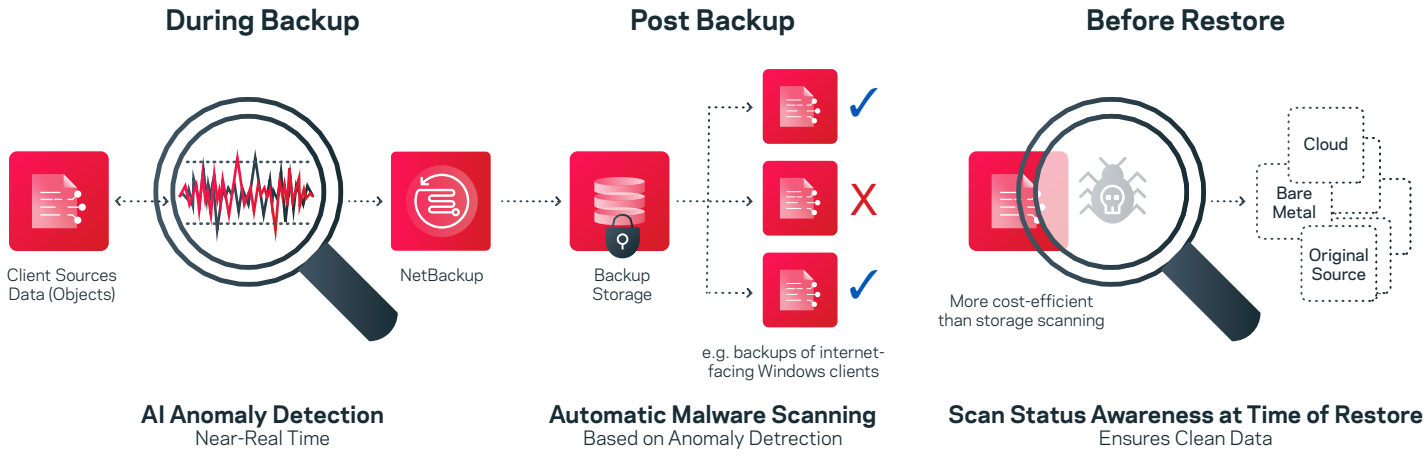


Figure 2. An overview of NetBackup's anomaly detection and malware scanning capabilities.

Multi-Cloud Optimized with Veritas Alta Data Protection

Veritas Alta™ Data Protection is the NetBackup component that provides coverage for cloud workloads. NetBackup 10.1 and 10.2 greatly expanded support for platform-as-a-service (PaaS) workloads, adding protection for 15 new workloads across three cloud providers. Veritas Alta Data Protection fully supports highly flexible cloud workloads, empowering you to transport workloads from providers into the MSDP storage pools, optimizing and deduplicating data, and using efficient object storage to simplify recovery. Cloud data is now available directly from backup storage so users can view compressed, encrypted, and deduplicated data.

NetBackup 10.3 further expands functionality with support for more PaaS workloads, including:

- AWS Amazon Relational Database Service — Oracle
- Google Cloud Platform Cloud SQL for SQL Server
- Microsoft Azure Cosmos DB – Mongo and SQL API
- Microsoft Azure Data Lake

This brings the total to 20, with more to come in future updates. Incremental backup support is available for Azure SQL and Azure SQL MI, protecting Azure SQL workloads with minimal overhead, compute, and storage requirements.

Veritas Alta Data Protection is powered by Cloud Scale Technology, which delivers enhanced protection and simplified operations across expanded workloads, including Kubernetes and software-as-a-service–based (SaaS-based) applications. It provides secure, automated, and orchestrated workload protection, resulting in a more cost-effective, resilient, and sustainable environment with:

- Elastic backup and recovery services for AWS and Azure
- Agentless backup from snapshot
- Enhanced elastic cloud autoscaling for AWS and Azure
- Elastic cloud deduplication services

Automated Operations

With automated and intelligent policies, NetBackup enhances protection and simplifies operations for the broadest collection of workloads to date, including traditional, PaaS, SaaS, and container-based applications. It provides secure, resilient, orchestrated delivery of intelligent, event-driven workload protection at the edge, on-premises, and in the cloud. Reduce data-protection gaps by minimizing human error and time-consuming administrative tasks with new capabilities, including:

- Integration with cloud-based SIEM/SOAR for Azure Sentinel
- Integrated SaaS application data protection
- Integrated multi-cloud analytics and insights
- Kubernetes multi-cloud recovery
- Enhanced media server elasticity and intelligence
- Expanded Amazon S3 immutability support

NetBackup 10.3 also introduces enhanced media server elasticity and intelligence to optimize resource utilization and cost savings. NetBackup automatically optimizes spin-up to incrementally improve efficiency by deploying the smallest media server image required for the demand. This reduces total utilization to keep compute costs at the lowest possible level.

NetBackup 10.3 expands support to include the market's widest range of certified S3 and integrated object-level lock targets, providing full deduplication and optimization from any workload to any target (Figure 3).

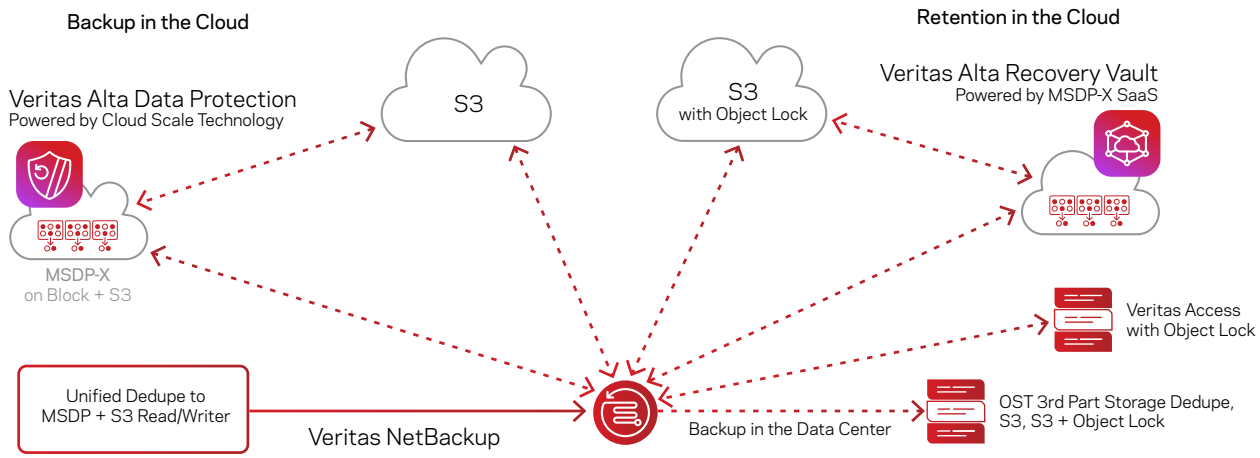


Figure 3. Overview of Veritas NetBackup cloud workload support

Veritas Alta SaaS Protection

Veritas Alta SaaS Protection enables you to back up and recover SaaS application data from any major SaaS offering. This includes Box, Google Workspace, Microsoft 365, Salesforce, and Slack—more than any other vendor (Figure 4).

Veritas Alta SaaS Protection provides fully managed, automated backups that run according to the policies you configure. Unlike other vendors' products, its built on a single-tenant architecture, giving your organization its own dedicated instance. Your data remains completely isolated, and you receive a dedicated set of cloud resources, ensuring high performance. This provides short recovery point objectives (RPOs), minimizing the data that can be lost through deletion—accidental or malicious—or to a ransomware attack.

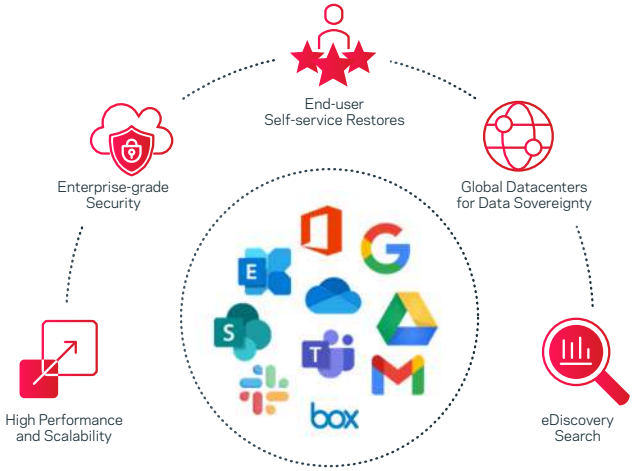


Figure 4. NetBackup protects data across a variety of SaaS applications and environments.

Veritas Alta SaaS Protection provides automatic compliance enforcement by allowing you to set policies for data retention and data location controls. It offers flexible recovery options, from bulk to single-item restores. And Veritas Alta SaaS Protection integrates with NetBackup, allowing you to monitor the status of backup jobs from the NetBackup web UI console.

Veritas Alta Recovery Vault

Veritas Alta Recovery Vault is a cloud-based data-retention service that provides a seamless, fully managed secondary storage option for NetBackup users (Figure 5).

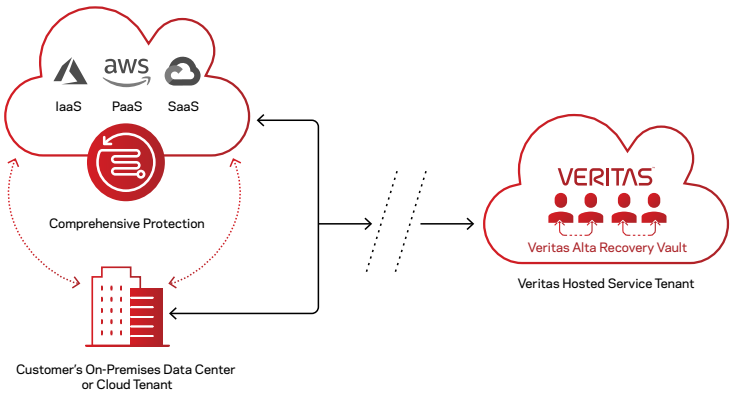


Figure 5. Veritas Alta Recovery Vault provides storage for data across on-premises and cloud

Veritas Alta Recovery Vault and the Intelligent Cloud Policy Engine ensure that no data is left behind. Multi-cloud isolation provides complete protection from ransomware and other threats. All this is accomplished through a simplified process within the familiar NetBackup UI.

Use Veritas Alta Recovery Vault to safely store anything that you protect with NetBackup or Veritas Alta Data Protection. With Veritas Alta Recovery Vault, you can plan for disaster recovery, meet compliance and governance requirements, and prevent data loss from ransomware.

Veritas Alta Recovery Vault also offers a token-based authentication feature that maintains a cloud-based air gap in Azure or AWS to ensure complete security of your data from external threats.

Integrated NetBackup IT Analytics Foundation

Introduced in NetBackup 10, the Integrated NetBackup IT Analytics Foundation delivers capabilities to connect cloud and information for data insights and provide intelligence across hybrid and multi-cloud environments. NetBackup 10.1 added the ability to use information to optimize performance and mitigate risk. By pinpointing operational inefficiencies, identifying threshold-based backup inconsistencies, and compiling a single-source report, NetBackup can easily identify necessary changes to make (Figure 6).

Figure 6. Example of NetBackup IT Analytics Foundation's single-source report bringing together cloud and information insights

Using these analytics reduces overall cloud costs through rightsizing and optimizing cloud infrastructure. Unifying insights from multiple cloud service providers helps you identify exact costs and consolidate public-cloud expenditures for further analysis and action.

Kubernetes Multi-Cloud, Multi-Distribution Recovery

NetBackup provides the industry's broadest support for Kubernetes with the consistency and portability you need to protect any Kubernetes distribution, on-premises or in the cloud. Veritas designed NetBackup for Kubernetes to offer operational simplicity and enterprise-grade resiliency with choice and flexibility for workload protection.

Back up Kubernetes workloads to any available storage target in the NetBackup web UI. For cloud, Kubernetes data protection operations are effectively managed with NetBackup's elastic cloud autoscaling, dynamically provisioning and removing cloud instances as needed to maximize cost and efficiency. In addition, it includes built-in features for:

- Instant rollback from snapshots
- Application-consistent Kubernetes cluster backup
- Deduplication
- Image duplication for tiering backup storage service lifecycle policies (SLPs)
- Auto image replication (AIR)

NetBackup 10.3 extends CSI-based snapshot support for block-based and file-based storage in the same namespace. This allows for parallel stream recovery and up to a 218% performance gain in restore speeds. These Kubernetes capabilities are fully integrated with all NetBackup ransomware resiliency functionality to ensure data is always recoverable.

NetBackup for Kubernetes features simplified installation, configuration, and management. Intelligent policies dynamically discover all namespaces and their labels on the Kubernetes cluster, plus use customer-defined parameters to add namespaces to the protection plan. This ensures automatic protection, reduces risk of data loss, and gives you much greater control in defining how you protect your applications, providing the ability to easily include and exclude specific resources.

More than 50% of organizations using Kubernetes run more than one distribution. Portability is one of the biggest drivers of Kubernetes adoption, specifically the ability to move between on-premises and different clouds. NetBackup provides the freedom to run as many distributions of Kubernetes as you need, without requiring different backup products.

Why Veritas?

Veritas NetBackup and Veritas Alta Data Protection provide cost-effective and secure sustainability to your enterprise hybrid cloud. The solution uniquely integrates SaaS, analytics, and automated on-demand services, protecting data while improving operational agility and control across any cloud.

Today's environments require you to manage data as a key asset and ensure rapid recovery of critical data during catastrophic events such as lost files, security attacks, or unexpected business disruptions.

Learn more about **NetBackup** and **Alta Data Protection**.

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 91 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1512 10/23

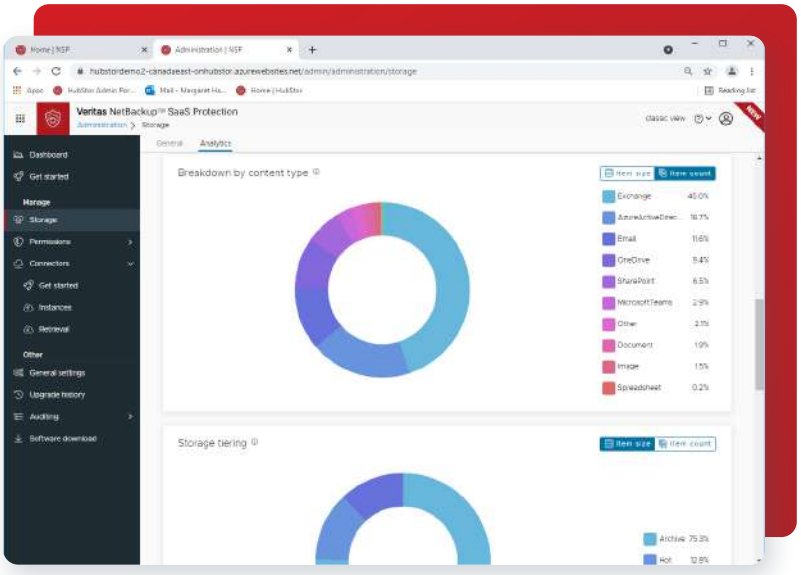
VERITAS

Veritas Alta SaaS Protection

Enterprise-grade performance and scale for protection of SaaS application data.

Software-as-a-Service (SaaS) applications, once the exception, have become the standard approach for many enterprises. Maintaining these applications is usually less expensive and far simpler than managing on-premises applications, as the SaaS provider takes care of all the infrastructure as well as the application software.

However, under the Shared Responsibility Model, SaaS application providers are not responsible for backing up customer data, which leaves it exposed to both ransomware attacks and the risk of deletion — whether accidental or malicious. The responsibility to protect SaaS application data falls entirely on the customer.



Veritas Has Your SaaS Application Data Covered

Protect the full range of data stored across your SaaS platforms. Ensure that your data is quickly and easily recoverable in the event of unplanned deletion or a ransomware attack. Veritas Alta™ SaaS Protection (formerly known as NetBackup SaaS Protection) supports:

- Microsoft 365
  - Exchange Online mailboxes, folders, messages, and attachments
  - SharePoint Online sites, folders, files, permissions, and metadata
  - OneDrive for Business sites, folders, files, permissions, and metadata
  - Teams users, teams, channels, messages, meeting recordings, and attachments
- Google Workspace
  - Gmail mailboxes, folders, labels, messages, and attachments
  - Google Drive files, folders, permissions, and metadata
  - Support for Docs, Slides, Sheets, Drawings, and other G-Suite applications
- Slack
  - Channels, users, messages, and attachments
- Box
  - Files, folders, permissions, and metadata
- Salesforce
  - Support for both key Salesforce product categories: Service Cloud and Sales Cloud
  - Protection for sandbox and productions organizations (orgs)
  - Protection for custom and standard objects, such as cases, accounts, contacts, leads, users, contracts, etc
  - Highly complex Salesforce object relationships automatically preserved during restore
  - Easily find Salesforce content to restore via the built-in query engine or using the recovery wizard

Protect More Than SaaS Data

In addition to SaaS application data, Veritas Alta SaaS Protection supports backup and recovery of Platform-as-a-Service (PaaS) data, including:

- Amazon Web Services (AWS) S3
- Microsoft Azure Blob Storage
- Microsoft Azure File Storage
- On-premises unstructured data

> *After Veritas Alta SaaS Protection writes the backups, they cannot be changed. We consider the backup and protection of our data to be one of our most important lines of defense [against] a ransomware attack—we are confident that our data is safe with Veritas."*
>
> **Nizar Radad, Head of IT,**
> Qatar Engineering & Construction Company

Prevent Data Loss with Reliable Backup and Flexible Recovery

Veritas Alta SaaS Protection backup-as-a-service (BaaS) lets you scale across regions and domains, back up continuously, and deliver the performance that ensures your backup never falls behind. Seamless integration with SaaS and PaaS APIs easily maintains a synthetic full backup of your data. Perform backup of entire data stores. Restore data at granular and bulk levels to the original or alternate locations. Use recovery to perform item-level restores.

In addition to backing up all data objects, Veritas Alta SaaS Protection also captures—and can restore—important metadata including permissions.

Full Control

You set your backup policies and permissions as well as the hosting cloud region, giving you full data residency control, making compliance with data sovereignty regulations simple. Rapidly export search results in the event of a legal discovery request or compliance audit.

Enterprise Security

Get secure storage for your backup data residing in a dedicated, SOC 2 Type II-compliant instance of the Veritas data management platform using end-to-end encryption, multi-factor authentication, and enhanced granular role-based access controls (RBAC).

Enterprise Scalability

SaaS and PaaS environments can grow to be exceptionally large, so you need a data protection solution that scales to grow with your organization. Veritas Alta SaaS Protection backup storage can grow as needed, easily scaling to multiple petabytes and billions of objects.

Ransomware Protection

Protects against data loss from modern cybersecurity threats, such as ransomware.

Flexible Recovery

Deep backup and restore capabilities for core enterprise Microsoft 365 applications.

Single-Tenant Solution

Industry-leading security architecture built and tailored for the needs of large enterprises.

Scalability

Best-in-class performance, scalability, and security for large enterprises.

Data Sovereignty

Dedicated tenancy and multi-geo support enable control over data sovereignty.

Market Leadership

Veritas Alta SaaS Protection suite of solutions is the leader in the enterprise data protection market.

How Veritas Delivers Leading SaaS Application Data Protection

Backup Coverage	Recovery Options	Security	Platform
Microsoft 365	Granular restore	Immutable storage	Software-as-a-service (SaaS)
Google Workspace	Bulk restores	IP allow / deny lists	Data residency controls
Slack	Point-in time restore	End-to-end encryption	Flexible deployment options
Box	Choice of restore location	Multi-Factor Authentication	Multi-region support
Amazon S3	Package data for export	Single sign-on (SSO)	Multi-domain support
Azure Blob and File Storage	Low recovery time objectives (RTOs)	Access control lists (ACLs)	Petabyte scalability
Low recovery point objectives (RPOs)	Provides ransomware resiliency	Enhanced role-based access control (RBAC)	Unlimited data retention
Veritas Alta SaaS Protection			

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1596 08/23

NetBackup Appliances

	VERITAS				
Metrics	5260	5360	Flex Scale 4 Node	Flex Scale 8 Node	Flex Scale 16 Node
Max Throughput TB/hr (Distributed Dedupe)	207	228	265	503	1037
Max Throughput TB/hr (Server Side Dedupe)	31	73	84	145	282
High Availability (HA)	No	Active/Active	Scale Out	Scale Out	Scale Out
Maximum Usable Capacity TB	441	1,920	448	896	1792
Storage Density TB/U	31 (14U)	87 (22U)	56 (8U)	56 (16U)	56 (32U)
Power Consumption W/TB (Typical)	4.4	2.5	3.1	3.1	3.1
Integrated vs Target Appliance	Integrated	Integrated	Integrated	Integrated	Integrated
Off-host Dedupe DB Protection	Yes	Yes	Yes	Yes	Yes
Private Cloud Long Term Retention	Access 3340	Access 3340	Access 3340	Access 3340	Access 3340
Deduplication to Cloud	No additional license, no gateway required	No additional license, no gateway required	No additional license, no gateway required	No additional license, no gateway required	No additional license, no gateway required

BRASIL

INMETRO

- - - - - - - - Site do Inmetro - - - - - - - -

Sites de Interesse | Mapa do Site | Ouvidoria | Fale com o Inmetro

Certificados | Produtos | Serviços | Empresas | Organismos Acreditados

voltar

Produtos e Serviços com Conformidade Avaliada

Certificados

Resultado da Consulta:
9 Certificado(s)
16 Produtos(s)
0 Serviços(s)

Página 1

Certificador: IEX Nº Certificado: IEX 14.0301R3.F2.2 Tipo: Produto Emissão: 02/11/2022 Validade: 01/11/2025 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
22357186000173	VERITAS TECNOLOGIA (BRASIL) LTDA		AVENIDA DAS NAÇÕES UNIDAS, 14261 - ANDAR 28 - VILA GERTRUDES - SÃO PAULO, SP - BRASIL	ATIVO	REPRESENTANTE LEGAL
	SEAGATE CLOUD SYSTEMS, INC.	SEAGATE (USA)	47488 KATO RD., - - - 94538 - FREMONT - CA, - ESTADOS UNIDOS	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
SEAGATE	HB-1235.	SIM	UNIDADE DE ARMAZENAMENTO DE DADOS - 100 - 240 VCA; 8.0 - 3.0 A TOTAL; 50 / 60 HZ, CLASSE I
SEAGATE	HB-1235..	SIM	UNIDADE DE ARMAZENAMENTO DE DADOS - 100 - 240 VCA; 9.0 - 3.8 A TOTAL; 50 / 60 HZ, CLASSE I
SEAGATE	HB-1235...	SIM	UNIDADE DE ARMAZENAMENTO DE DADOS - -48 TO -60 VDC; 15.0 - 8.0 A OR 15.0 - 12.0 A

Certificador: IEX Nº Certificado: IEX 17.0130R2 Tipo: Produto Emissão: 27/10/2023 Validade: 26/10/2026 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
22357186000173	VERITAS TECNOLOGIA (BRASIL) LTDA		AVENIDA DAS NAÇÕES UNIDAS, 14261 - ANDAR 28 - VILA GERTRUDES - SÃO PAULO, SP - BRASIL	ATIVO	REPRESENTANTE LEGAL
	NETWORK ENGINES, INC.	NETWORK (CANTON)	25 DAN ROAD, - - - 02021-2817 CANTON MA, - ESTADOS UNIDOS	ATIVO	SOLICITANTE

Marca	Modelo	Importado	Descrição
VERITAS	VER5000WF	SIM	UNIDADE DE ARMAZENAMENTO E PROCESSAMENTO DE DADOS / SERVIDOR - 100-127 / 200-240 V~; 10 / 5 A (X2); 50 / 60 HZ
VERITAS	VER5000WFE	SIM	UNIDADE DE ARMAZENAMENTO E PROCESSAMENTO DE DADOS / SERVIDOR - 100-127 / 200-240 V; 8,5 / 5,0 A (X2) ~; 50 / 60 HZ

Certificador: IEX Nº Certificado: IEX 17.0133R2 Tipo: Produto Emissão: 27/10/2023 Validade: 26/10/2026 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa

topo

22357186000173	VERITAS TECNOLOGIA (BRASIL) LTDA		AVENIDA DAS NAÇÕES UNIDAS, 14261 - ANDAR 28 - VILA GERTRUDES - SÃO PAULO, SP - BRASIL	ATIVO	REPRESENTANTE LEGAL
	NETWORK ENGINES, INC.	NETWORK (CANTON)	25 DAN ROAD, - - - 02021-2817 CANTON MA, - ESTADOS UNIDOS	ATIVO	SOLICITANTE

Marca	Modelo	Importado	Descrição
VERITAS	VER5000WF	SIM	UNIDADE DE ARMAZENAMENTO E PROCESSAMENTO DE DADOS / SERVIDOR - 100-127 / 200-240 V~; 10 / 5 A (X2); 50 / 60 HZ
VERITAS	VER5000WFE	SIM	UNIDADE DE ARMAZENAMENTO E PROCESSAMENTO DE DADOS / SERVIDOR - 100-127 / 200-240 V; 8,5 / 5,0 A (X2) ~; 50 / 60 HZ

Certificador: IEX Nº Certificado: IEX 18.0013R1.F2 Tipo: Produto Emissão: 27/02/2021 Validade: 26/02/2024 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
22357186000173	VERITAS TECNOLOGIA (BRASIL) LTDA		AVENIDA DAS NAÇÕES UNIDAS, 14261 - ANDAR 28 - VILA GERTRUDES - SÃO PAULO, SP - BRASIL	ATIVO	REPRESENTANTE LEGAL
	NETWORK ENGINES, INC.	NETWORK (CANTON)	25 DAN ROAD, - - - 02021-2817 CANTON MA, - ESTADOS UNIDOS	ATIVO	SOLICITANTE

Marca	Modelo	Importado	Descrição
SEAGATE	SP-2584 - 200-240 V~; 13 A; 50 / 60 HZ; CLASSE I	SIM	UNIDADE DE ARMAZENAMENTO DE DADOS
SEAGATE	SP-2584 - 200-240 V~; 16 A; 50 / 60 HZ; CLASSE I	SIM	UNIDADE DE ARMAZENAMENTO DE DADOS

Certificador: IEX Nº Certificado: IEX 19.0093R1.F18 Tipo: Produto Emissão: 10/06/2022 Validade: 09/06/2025 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
22357186000173	VERITAS TECNOLOGIA (BRASIL) LTDA		AVENIDA DAS NAÇÕES UNIDAS, 14261 - ANDAR 28 - VILA GERTRUDES - SÃO PAULO, SP - BRASIL	ATIVO	REPRESENTANTE LEGAL
	NETWORK ENGINES, INC.	NETWORK (CANTON)	25 DAN ROAD, - - - 02021-2817 CANTON MA, - ESTADOS UNIDOS	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
VERITAS	VER5000WF0	SIM	UNIDADE DE ARMAZENAMENTO E PROCESSAMENTO DE DADOS / SERVIDOR - 100-127 / 200-240 V~; 50 / 60 HZ; 10 / 5 A (X2) OR 100-127 / 200-240 V~; 50 / 60 HZ; 8,5 / 7,5 A (X2)
VERITAS	VER5000WF0E	SIM	UNIDADE DE ARMAZENAMENTO E PROCESSAMENTO DE DADOS / SERVIDOR - 100100-127 / 200-240 V~; 50 / 60 HZ; 8,5 / 7,5 A (X2)

Certificador: IEX Nº Certificado: IEX 19.0093R1.F22 Tipo: Produto Emissão: 10/06/2022 Validade: 09/06/2025 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
22357186000173	VERITAS TECNOLOGIA (BRASIL) LTDA		AVENIDA DAS NAÇÕES UNIDAS, 14261 - ANDAR 28 - VILA GERTRUDES - SÃO PAULO, SP - BRASIL	ATIVO	REPRESENTANTE LEGAL
	NETWORK ENGINES, INC.	NETWORK (CANTON)	25 DAN ROAD, - - - 02021-2817 CANTON MA, - ESTADOS UNIDOS	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
VERITAS	VER5000WF0	SIM	UNIDADE DE ARMAZENAMENTO E PROCESSAMENTO DE DADOS / SERVIDOR - 100-127 / 200-240 V~; 50 / 60 HZ; 10 / 5 A (X2) OR 100-127 / 200-240 V~; 50 / 60 HZ; 8,5 / 7,5 A (X2)

VERITAS	VER5000WF0E	SIM	UNIDADE DE ARMAZENAMENTO E PROCESSAMENTO DE DADOS / SERVIDOR - 100100-127 / 200-240 V~; 50 / 60 HZ; 8,5 / 7,5 A (X2)

Certificador: IEX Nº Certificado: IEX 23.0090.F18 Tipo: Produto Emissão: 23/05/2023 Validade: 22/05/2026 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
22357186000173	VERITAS TECNOLOGIA (BRASIL) LTDA		AVENIDA DAS NAÇÕES UNIDAS, 14261 - ANDAR 28 - VILA GERTRUDES - SÃO PAULO, SP - BRASIL	ATIVO	REPRESENTANTE LEGAL
	NETWORK ENGINES, INC.	NETWORK (CANTON)	25 DAN ROAD, - - - 02021-2817 CANTON MA, - ESTADOS UNIDOS	ATIVO	SOLICITANTE

Marca	Modelo	Importado	Descrição
VERITAS	VER5000CYP	SIM	UNIDADE DE ARMAZENAMENTO E PROCESSAMENTO DE DADOS / SERVIDOR 100100-127 / 200-240 V~; 50 / 60 HZ; 8,5 / 7,5 A (X2)

Certificador: IEX Nº Certificado: IEX 23.0090.F22 Tipo: Produto Emissão: 23/05/2023 Validade: 22/05/2026 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
22357186000173	VERITAS TECNOLOGIA (BRASIL) LTDA		AVENIDA DAS NAÇÕES UNIDAS, 14261 - ANDAR 28 - VILA GERTRUDES - SÃO PAULO, SP - BRASIL	ATIVO	REPRESENTANTE LEGAL
	NETWORK ENGINES, INC.	NETWORK (CANTON)	25 DAN ROAD, - - - 02021-2817 CANTON MA, - ESTADOS UNIDOS	ATIVO	SOLICITANTE

Marca	Modelo	Importado	Descrição
VERITAS	VER5000CYP	SIM	UNIDADE DE ARMAZENAMENTO E PROCESSAMENTO DE DADOS / SERVIDOR 100100-127 / 200-240 V~; 50 / 60 HZ; 8,5 / 7,5 A (X2)

Certificador: UL Nº Certificado: UL-BR 23.0306 Tipo: Produto Emissão: 20/07/2023 Validade: 19/07/2026 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
22357186000173	VERITAS TECNOLOGIA (BRASIL) LTDA		AVENIDA DAS NAÇÕES UNIDAS, 14261 - ANDAR 28 - VILA GERTRUDES - SÃO PAULO, SP - BRASIL	ATIVO	SOLICITANTE

Marca	Modelo	Importado	Descrição
VERITAS	E03J	SIM	EQUIPAMENTO PARA ARMAZENAMENTO DE DADOS / I/P: 8.6A 100-240V~ 50/60HZ OR 25A – (48-60) V DC, CLASS I

Veritas™ 5260 Appliance Product Description Guide

VERITAS™

Veritas 5260 Appliance Product Description Guide

Last updated: 2023-10-13

Document version: Revision 1.0

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://www.veritas.com/content/support/en_US/dpp.Appliances.html

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

APPL.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1 About the Veritas 5260 Appliance 6

Veritas 5260 Appliance overview 6
Features and components of the Veritas 5260 Appliance 8
Locating the appliance serial number 10
Veritas 5260 Appliance front panel drive configurations 11
About the drive LEDs 12
About the Veritas 5260 Appliance front panel USB port 13
About the 5260 Appliance control panel 13
About the System Status LED states 16
About the Power button LED states 19
About the 5260 Appliance rear panel 20
Veritas 5260 Appliance I/O configuration options 22
Veritas 5260 Appliance total I/O on-board and PCIe ports 25
Customizable I/O configurations by slot for existing Veritas 5260 Appliance 25
Broadcom P225p 10/25Gb PCIe Ethernet card 26
QLE2772 dual-port 32 Gb Fibre Channel host bus adapter 27
Intel RAID Adapter RS3P4MF088F 29

Chapter 2 Veritas 2U12 65.5TiB/72TB Storage Shelf 31

Storage Shelf overview 31
Usable appliance storage capacities 32
Components of the Storage Shelf 33
Storage Shelf front panel components 33
Storage Shelf control panel 35
Storage Shelf rear components 38
Storage Shelf I/O modules 39
I/O module Status LED location and conditions 41
I/O module SAS Activity LED location and conditions 41
Storage Shelf Power Cooling Modules 42
Power Cooling Module LEDs 44

Chapter 3 Veritas 5260 Appliance and Veritas 2U12 65.5TiB/72TB Storage Shelf cables 46

Power cables 46
Network cable 47
Multi-Mode fiber optic cable 48
Twinaxial copper cables 49
SAS-3 cable 50

Appendix A Technical specifications, Environmental/Protocol standards, and Compliance standards 52

Veritas 5260 Appliance technical specifications 52
Veritas 2U12 65.5TiB/72TB Storage Shelf technical specifications 55
Environmental specifications 57
Protocol standards 58
Regulatory, compliance, and certification information 58
Product regulatory compliance 59
Country approvals 59
Product safety compliance 60
Product EMC Compliance - Class A Compliance 60
Product environmental compliance 61

Index 62

Chapter 1

About the Veritas 5260 Appliance

This chapter includes the following topics:

- Veritas 5260 Appliance overview
- Features and components of the Veritas 5260 Appliance
- Locating the appliance serial number
- Veritas 5260 Appliance front panel drive configurations
- About the Veritas 5260 Appliance front panel USB port
- About the 5260 Appliance control panel
- About the 5260 Appliance rear panel
- Veritas 5260 Appliance I/O configuration options

Veritas 5260 Appliance overview

The Veritas 5260 Appliance is a hardware and software storage system that can scale to 429.4 TiB of available backup capacity. It consists of a Veritas 5260 Appliance and up to six optional Veritas 2U12 65.5TiB/72TB storage shelves. By itself, the 2U Veritas 5260 Appliance offers internal storage from 9.1 TiB to 36.4 TiB, depending on the appliance configuration purchased.

Figure 1-1 Veritas 5260 Appliance

A Veritas 2U12 storage shelf offers 65.5 TiB of storage. Attaching six storage shelves offers 429.4 TiB of storage. As with previous generations of the Flex 52xx appliances, the Veritas 5260 Appliance can be configured as a primary server or a media server. It can also be configured as both. The 5260 Appliance supports upto 6 storage shelves.

See "Usable appliance storage capacities" on page 32.

SAS-3 cables connect the Veritas 5260 Appliance to the storage shelves. SAS-3 cables also connect the storage shelves to each other.

The Veritas 5260 Appliance supports the following software:

- Flex Appliance 3.2 and above

About Veritas 5260 Appliance configurations

To determine the right Veritas 5260 Appliance system for your environment, you should consider the environment's future storage requirements over the lifetime of the system.

Veritas offers multiple I/O configurations from which to choose. You can use the supported Veritas 5260 Appliance I/O configurations to best serve the needs of your particular environment.

These configurations include the following:

- One Veritas 5260 Appliance with 9.1 TiB of internal storage only
- One Veritas 5260 Appliance with 36.4 TiB of internal storage only
- One Veritas 5260 Appliance with up to six external 65.5TiB/72TB storage shelves for a total of 429.4 TiB of storage

If your environment requires more than 36TiBs of storage, consider the Veritas 5260 Appliance with 9.1TiBs of internal storage and one 65.5TiB/72TB Veritas 2U12 65.5TiB/72TB Storage Shelf. If more storage is required, you can add up to five additional storage shelves to this configuration.

Features and components of the Veritas 5260 Appliance

This section describes the features and components of the Veritas 5260 Appliance.

Table 1-1 Veritas 5260 Appliance features

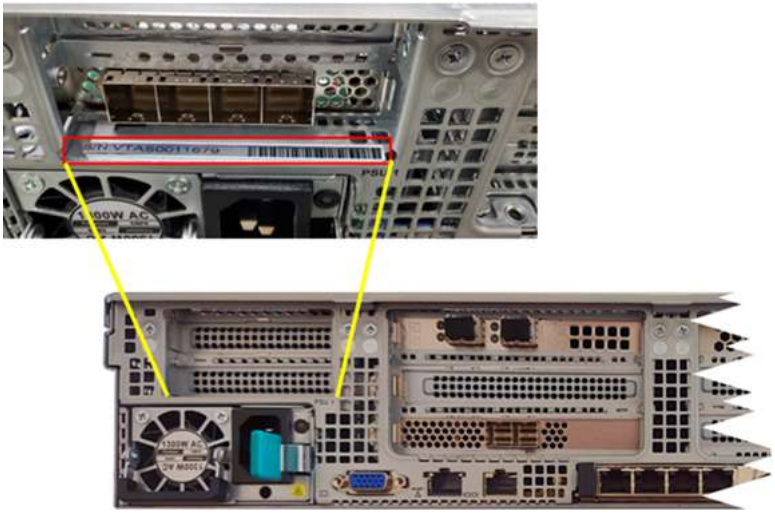
Feature	Description
Processor	Intel Xeon Scalable Third generation Silver 4314
Appliance software version	Flex Appliance 3.2 or higher
Performance and capacity	■ Supports high-performance processors with low-power consumption. ■ Provides high-capacity intra-appliance switching bandwidth, along with high I/O throughput. ■ Available internal storage capacities of 9 TB, or 36 TB without optional external storage shelves. The available capacity can be allocated either in part or in whole to a deduplication pool or to an AdvancedDisk pool (non-deduplicated storage).
System memory configuration (DIMMS)	64GB, up to a maximum of 512GB **Note:** When you purchase the first expansion storage shelf, the Storage Expansion kit that comes with the storage shelf includes a replacement of 256GB memory. A Memory Expansion kit containing eight 32GB DIMM memory chip is needed to support the fifth storage shelf.
Space reduction	The deduplication engine provides up to 100 times reduction in storage. The client-side plug-in provides similar levels of bandwidth reduction.
Scalable architecture	Due to fingerprinting and RAID redundancy, the overall storage capabilities are not a simple multiplication of the disk size and the total number of disks.
High availability	Supports redundant hot-swappable disks and power modules.

Table 1-1 Veritas 5260 Appliance features *(continued)*

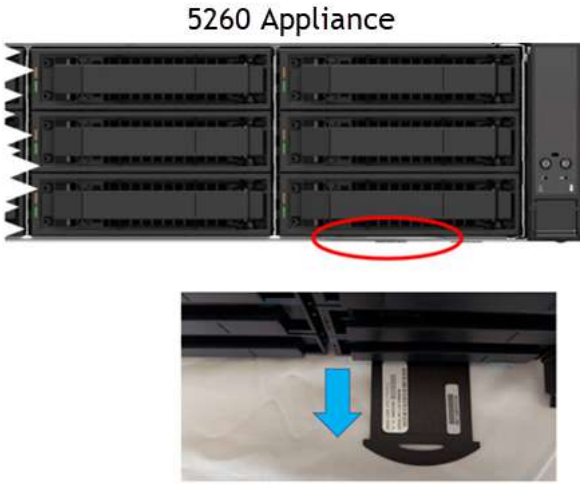
Feature	Description	
RAID levels	RAID 1 (standard mirroring) and RAID 6 (block level striping with double distributed parity) are implemented as follows: ■ Appliance system disks: RAID 1 ■ Appliance storage disks: RAID 6 ■ Storage shelf data storage disks: RAID 6 **Note:** The disk drives in the appliance are pre-formatted before the appliance is shipped. These drives should not be moved into different slots or otherwise rearranged.	
Fibre Channel support	The Veritas 5260 Appliance can be ordered with one, two, three or four PCIe 32 Gb Fibre Channel host bus adapter cards preinstalled. See " Veritas 5260 Appliance I/O configuration options" on page 22. See "Customizable I/O configurations by slot for existing Veritas 5260 Appliance" on page 25.	
PCIe 10/25 Gb Ethernet cards	Yes (with Fibre Optic ports)	
I/O Ports See "Veritas 5260 Appliance total I/O on-board and PCIe ports" on page 25.	12 Gb SAS-3 ports (PCIe-based) (RAID controller)	2 Used to connect the Veritas Appliance compute node to the 2U12 Primary Storage Shelf
	10/25 GbE Ethernet/iSCSI-capable ports (PCIe-based)	Up to six, depending on the appliance I/O configuration
	32 Gb Fibre Channel ports (PCIe-based)	Up to eight, depending on the appliance I/O configuration
	10 Gb Ethernet ports (on-board)	4
Additional storage	Yes You can attach up to six optional storage shelves to the Veritas 5260 Appliance. Depending on the appliance configuration you purchase, a total of 429.4 TB of usable storage capacity is available. See "Usable appliance storage capacities" on page 32.	

Locating the appliance serial number

The serial number is located on the rear panel of the appliance above PSU 1 and begins with letters VTAS.



The serial number can also be found on the pull-out tab on the front of the appliance.



Veritas 5260 Appliance front panel drive configurations

The Veritas 5260 Appliance contains 3 NVMe solid state drives, and 8 SAS hard disk drives, which can be accessed from the appliance's front panel.

Figure 1-2 Appliance front panel drive slot assignments

The drives that are located in slot 4 and slot 5 are configured as the RAID1, VOLUME0 device. These drives contain the appliance operating system and the Flex application along with the log files. You can hot-swap one of these drives at a time; however, you cannot operate the appliance if both drives are removed.

The drive in slot 6 acts as a hot spare for OS and log files.

The drives in slots 0-3 and slots 8-10 store user data. They are configured as a RAID 6 array, which uses block-level striping with two parity blocks across each of the drives in the volume.

The appliance uses the drive that is located in slot 11 as a hot-spare drive. If one of the drives fails in slots 0-3 or slots 8-10, the appliance automatically initiates a RAID 6 rebuild operation. It rebuilds the RAID 6 array by using the hot-spare drive in slot 11. After you replace the failed drive, the appliance then copies the information from the drive in slot 11 to the new replacement drive. When the copy operation finishes, the drive in slot 11 again becomes the hot-spare drive.

Note: The hot-spare drive size depends on the data drive size.

Warning: The drives are pre-formatted before the appliance is shipped. Do not rearrange the drives from their original locations.

Table 1-2 Veritas 5260 Appliance front panel drive configurations

Slot	RAID Configuration	Drive size	Drive role
0-3 8-10	RAID 6	2TB (Available internal storage is 9.1TiB) 8TB (Available internal storage is 36.4TiB)	User data
4,5	RAID 1	1.92 TB	OS/log files
6	RAID 1	1.92 TB	Hot spare for OS and log drives
11	RAID 6	2TB 8TB	Hot spare for user storage data

About the drive LEDs

Figure 1-3 Appliance drive LEDs

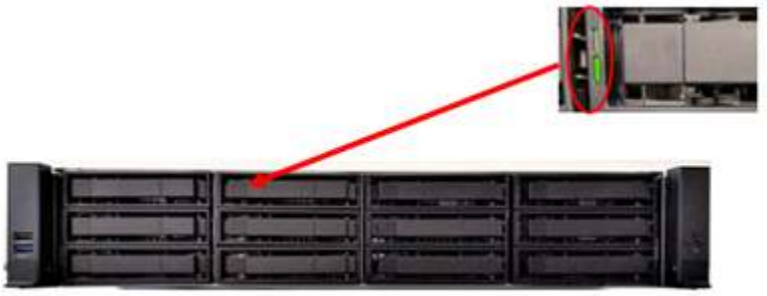


Table 1-3 Drive Status LED descriptions

Description	LED behavior	Condition
Amber Status LED	Off	No drive access and no disk drive faults
	Solid amber	A drive fault has occurred
	Blinking amber	A RAID rebuild is in progress (1Hz blink) Locating / identifying the drive (2Hz blink)

Table 1-4 Drive Activity LED States

Description	LED behavior	Condition
Green Activity LED	Off	Power on - the drive has spun down
	Solid green	Power on - no drive activity
	Blinking green	Power on - I/O is being processed by the drive or Power on - the drive is spinning up

About the Veritas 5260 Appliance front panel USB port

The Veritas 5260 Appliance front panel includes a USB 3.0-compliant port that supports a data transfer rate of up to 500 Mb/second.

About the 5260 Appliance control panel

The front control panel provides push button system controls and LED indicators for several system features.

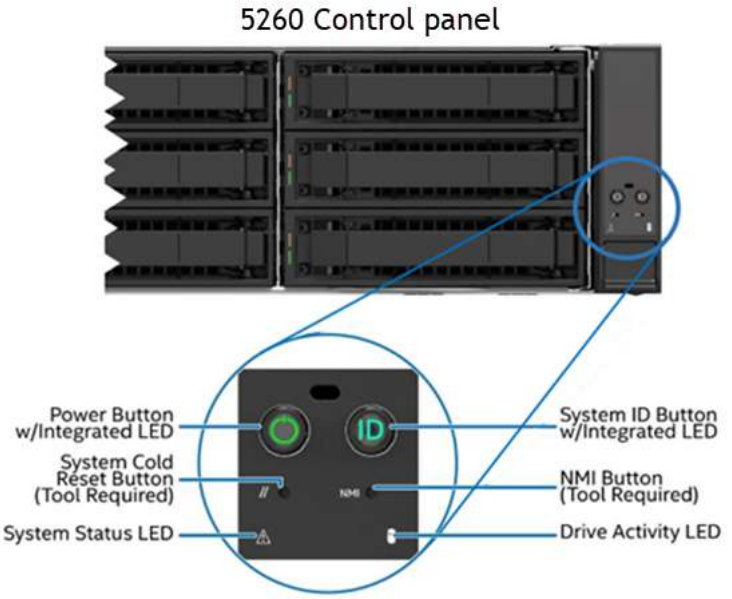


Table 1-5 Control panel system LED descriptions

LED	System information
Power button with integrated LED	The Power button toggles the system on and off. This button also functions as a sleep button if enabled by an ACPI compliant operating system. Pressing this button sends a signal to the integrated BMC that either powers on or powers off the system. Holding the power button for 10 seconds or more leads to a hard shutdown. The integrated LED is a single color (green) and supports different indicator states as defined in the following table. See "About the Power button LED states" on page 19.
Drive Activity LED	The drive activity LED on the front panel indicates drive activity from the server board SATA and sSATA storage controllers. The server board also has an I2C header labeled "SAS_MODULE_MISC" to provide access to this LED for add-in SATA or sSATA storage controllers.

Table 1-5 Control panel system LED descriptions *(continued)*

LED	System information
System ID button with integrated LED	Toggles the integrated ID LED and the blue server board system ID LED on and off. Both LEDs are tied together and show the same state. The onboard system ID LED is on the back edge of the server board, viewable from the back of the system. The system ID LEDs are used to identify the system for maintenance when installed in a rack of similar server systems. Two options available for illuminating the system ID LEDs are: ■ The front panel system ID LED button is pushed, which causes the LEDs to illuminate to a solid On state until the button is pushed again. ■ An IPMI `Chassis Identify` command is remotely entered that causes the LEDs to blink for 15 seconds.
NMI button (recessed, tool required for use)	When the NMI button is pressed, it puts the system in a halt state and issues a non-maskable interrupt (NMI). This situation can be useful when performing diagnostics for a given issue where a memory download is necessary to help determine the cause of the problem. To prevent an inadvertent system halt, the actual NMI button is behind the front control panel faceplate where it is only accessible with the use of a small tipped tool like a pin or paper clip.
System Cold Reset Button	When pressed, this button reboots and re-initializes the system. Unlike the power button, the reset button does not disconnect the power to the system. It just starts the system's Power-On Self-Test (POST) sequence over again.

Table 1-5 Control panel system LED descriptions *(continued)*

LED	System information
System Status LED	The system status LED is a bi-color (green/amber) indicator that shows the current health of the server system. The system provides two locations for this feature; one is on the front control panel and the other is on the back edge of the server board, viewable from the back of the system. Both LEDs are tied together and show the same state. The system status LED states are driven by the server board platform management subsystem. When the server is powered down (transitions to the DC-Off state or S5), the BMC is still on standby power and retains the sensor and front panel status LED state established before the power-down event. Two locations are provided for you to monitor the health of the system. You can find the first location on the front control panel, while the second location is located on the back edge of the server board. It is viewable from the rear of the appliance. Both LEDs show the same state of health. See "About the System Status LED states" on page 16.

About the System Status LED states

The following table provides a description of each LED state.

Table 1-6 System Status LED states

Color	State	Criticality	Description
No color	Off - The system is not operating.	Not ready	■ System power is off (AC and/or DC) ■ System is in EuP Lot6 Off Mode

Table 1-6 System Status LED states *(continued)*

Color	State	Criticality	Description
Green	Solid on (SO)	Healthy	■ System is in S5 Soft-Off State ■ Indicates that the system is running (in S0 State) and its status is “Healthy”. The system is not exhibiting any errors. AC power is present and BMC has booted and manageability functionality is up and running. ■ After a BMC reset, and with the chassis ID solid on, the BMC is booting Linux*. Control has been passed from BMC uBoot to BMC Linux*. The BMC is in this state for roughly 10–20 seconds.
Green	~1 Hz blink	Degraded The system is operating in a degraded state although still functional. or The system is operating in a redundant state but with an impending failure warning.	System degraded: ■ Redundant loss, such as power supply or fan. Applies only if the associated platform sub-system has redundancy capabilities. ■ Fan warning or failure when the number of fully operational fans is more than minimum number needed to cool the system. ■ Non-critical threshold crossed: Temperature (including HSBP temp), voltage, input power to power supply, output current for main power rail from power supply and Processor Thermal Control (Therm Ctrl) sensors. ■ Power supply predictive failure occurred while redundant power supply configuration was present. ■ Unable to use all of the installed memory (one or more DIMMs failed/disabled but functional memory remains available). ■ Battery failure ■ BMC executing in uBoot. (Indicated by Chassis ID blinking at 3Hz). System in degraded state (no manageability). BMC uBoot is running but has not transferred control to the BMC Linux. Server will be in this state 6-8 seconds after BMC reset while it pulls the Linux image into flash.

Table 1-6 System Status LED states *(continued)*

Color	State	Criticality	Description
Green	~1 Hz blink	Degraded (continued)	System degraded (continued): ■ BMC Watchdog has reset the BMC. ■ Power unit sensor offset for configuration error is asserted. ■ SSD Hot Swap Controller is off-line or degraded.
Green and amber altern atively	~1 Hz blink	System is initializing after source power is applied	■ PFR in the process of updating/authenticating/recovering when source power is connected, system firmware being updated. ■ System not ready to take power button event/signal.
Amber	~1 Hz blink	Non-critical The system is operating in a degraded state with an impending failure warning. However, the system is still functioning.	Non-fatal, although the system is likely to fail due to the following issues: ■ Critical threshold crossed – Voltage, temperature (including HSBP temp), input power to power supply, output current for main power rail from power supply and PROCHOT (Therm Ctrl) sensors. ■ VRD Hot asserted ■ Minimum number of fans to cool the system not present or failed ■ Hard drive fault ■ Power Unit Redundancy sensor – Insufficient resources offset (indicates not enough power supplies present) ■ In non-sparing and non-mirroring mode, if the threshold of correctable errors is crossed within the window. ■ Invalid firmware image detected during boot up or firmware update.

Table 1-6 System Status LED states *(continued)*

Color	State	Criticality	Description

Amber	Solid on	Critical, non-recoverable – System is halted	Fatal alarm – system has failed or shutdown:
			■ CPU CATERR signal asserted
			■ MSID mismatch detected (CATERR also asserts for this case)
			■ CPU0 is missing
			■ CPU Thermal Trip
			■ No power – power fault
			■ DIMM failure when there is only one DIMM present; no other good DIMM memory present
			■ Runtime memory uncorrectable error in non-redundant mode.
			■ DIMM Thermal Trip or equivalent
			■ BMC/Video memory test failed (Chassis ID shows blue/solid-on for this condition)
			■ SBB Thermal Trip or equivalent
			■ 240VA fault
			■ Both uBoot BMC FW images are bad (Chassis ID shows blue/solid-on for this condition)
			■ Fatal Error in processor initialization:
			  ■ Processor family not identical
			  ■ Processor model not identical
			  ■ Processor core/thread counts not identical
			  ■ Processor cache size not identical
			  ■ Unable to synchronize processor frequency
			  ■ Unable to synchronize QPI link frequency
			■ BMC fail authentication with non-recoverable condition, system hang at T-1; boot PCH only, system hang; PIT failed, system lockdown.

About the Power button LED states

The following table provides a description of each power state.

Table 1-7 Power button LED states

State	Power Mode	LED	Description
Power - off	Non-ACPI	Off	The system power is off, and the BIOS has not initialized the chipset.
Power - on	Non-ACPI	On	The system power is on and the green Power button LED is active.
S0	ACPI (Advanced Configuration and Power Interface)	Steady on	The system and the operating system are up and running.
S5	ACPI (Advanced Configuration and Power Interface)	Off	Mechanical is off and the operating system has not saved any context to the hard disk drive.

About the 5260 Appliance rear panel

The rear panel of the appliance has several access ports and other features, which are displayed in the following figures.

Figure 1-4 Veritas 5260 Appliance rear panel and connectors

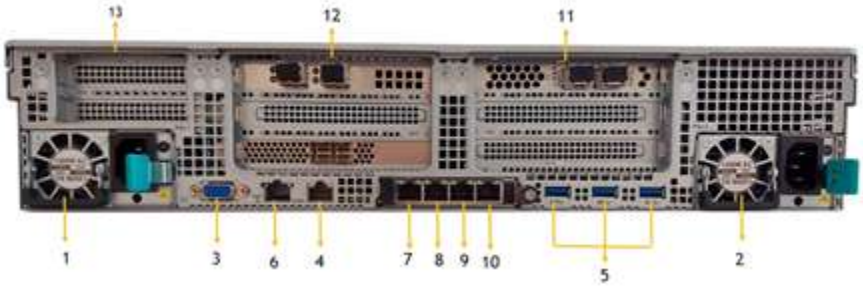


Table 1-8 Veritas 5260 Appliance rear panel features and connectors

Number	Function
1,2	Power Supply 1 and Power Supply 2 - Dual, redundant, and hot-swappable power supply modules
3	DB-15 VGA monitor connector

Table 1-8 Veritas 5260 Appliance rear panel features and connectors *(continued)*

Number	Function
4	Serial port - Serial connection for Veritas Technical Support use only
5	Three USB 3.0 ports for general use
6	IPMI port - An external RJ45 port used for appliance remote management purposes
7	Flex Appliance (host0): A 1-10 GbE port copper connector that you can connect to an administrative network to manage the appliance system. It is bonded during initial configuration as a standalone bond mgmt0.
8	Flex Appliance (NIC0): A 1-10 GbE port for general use.
9	Flex Appliance (NIC1): A 1-10 GbE port for general use.
10	Flex Appliance (NIC2): A 1-10 GbE port for general use.
11	PCIe riser assembly 1
12	PCIe riser assembly 2
13	PCIe riser assembly 3 Contains two half height PCIe slots. **Note:** PCIe riser assembly 2 and riser assembly 3 are riveted together. As a result, riser assembly 2 and riser assembly 3 are removed as one unit.

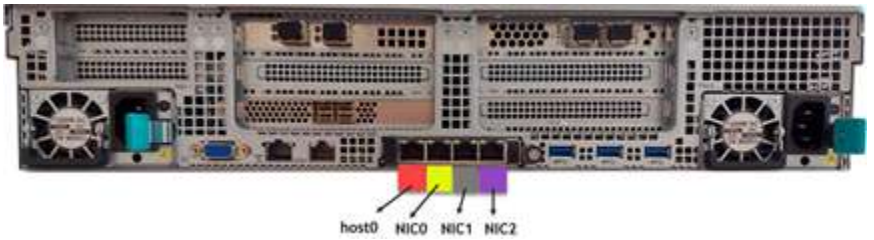
Note: You should not bond copper 1-10 Gb Ethernet ports that are installed in the appliance chassis with PCIe-based 10/25 Gb Ethernet Fibre Channel ports.

Veritas appliances may include grounding studs in case your lab environment has such a requirement. The studs are located on the rear panel of the appliance. You can use standard grounding practices to connect grounding wires to the studs.

The serial number is located on a vertical bar on the rear panel of the appliance.

The ports on the rear panel are color-coded for easy identification.

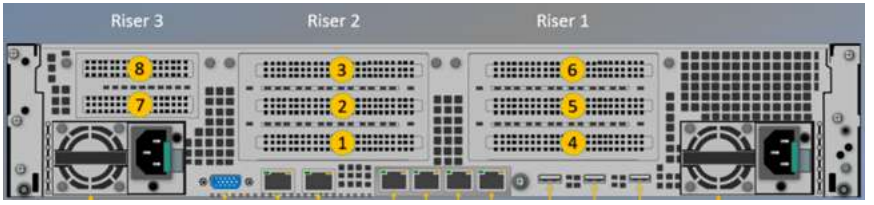
Figure 1-5 Veritas 5260 Appliance rear panel color codes



Veritas 5260 Appliance I/O configuration options

The rear panel of the Veritas 5260 Appliance contains three PCIe riser card assemblies. PCIe riser card assemblies 1 and 2 each support three standard PCIe cards, while PCIe riser card assembly 3 supports two low profile PCIe cards. The slots are labeled 1 to 8. Slots 1, 2, and 3 are located in PCIe riser card assembly 2. Slots 4, 5, and 6 are located in PCIe riser card assembly 1, while slots 7 and 8 are located in PCIe riser card assembly 3.

Figure 1-6 Rear panel riser assembly locations and PCIe slot number assignments



The Veritas 5260 Appliance supports multiple PCIe-based I/O configuration options. The following table shows the different I/O configuration options that are available.

Table 1-9 Available Veritas 5260 Appliance PCIe-based I/O configuration options

I/O configuration option	Slot 1 *	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8
A	-	-	10/25 GbE NIC	-	-	32 Gb FC HBA	-	-

Table 1-9 Available Veritas 5260 Appliance PCIe-based I/O configuration options *(continued)*

I/O configuration option	Slot 1 *	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8
B	-	10/25 GbE NIC	10/25 GbE NIC	10/25 GbE NIC	32 Gb FC HBA	32 Gb FC HBA	-	-
C	-	10/25 GbE NIC	10/25 GbE NIC	32 Gb FC HBA	32 Gb FC HBA	32 Gb FC HBA	-	-
D	-	32 Gb FC HBA	10/25 GbE NIC	32 Gb FC HBA	32 Gb FC HBA	32 Gb FC HBA	-	-

* Slot 1 contains a factory installed PCIe RAID controller

Figure 1-7 Flex 5260 Model A

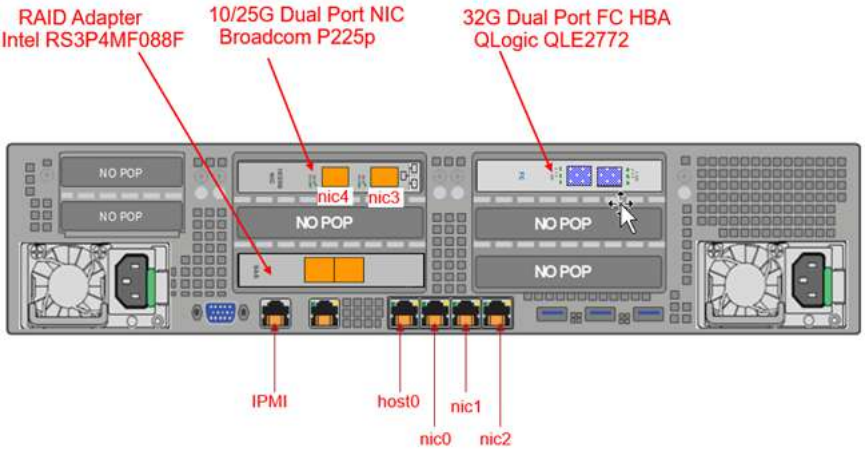


Figure 1-8 Flex 5260 Model B

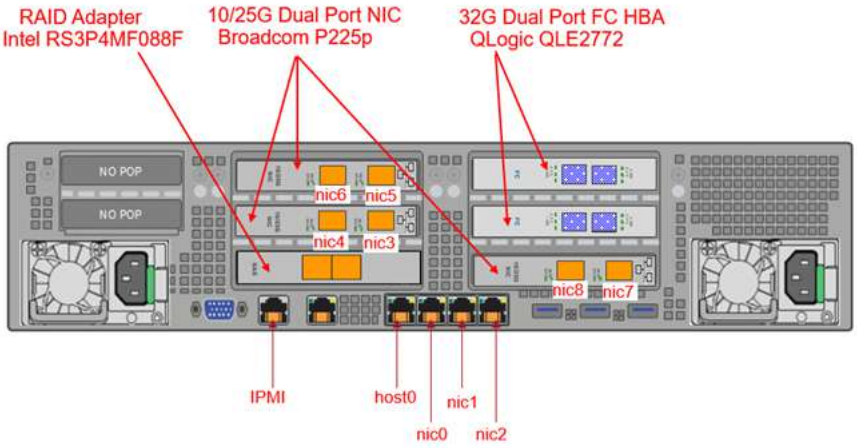


Figure 1-9 Flex 5260 Model C

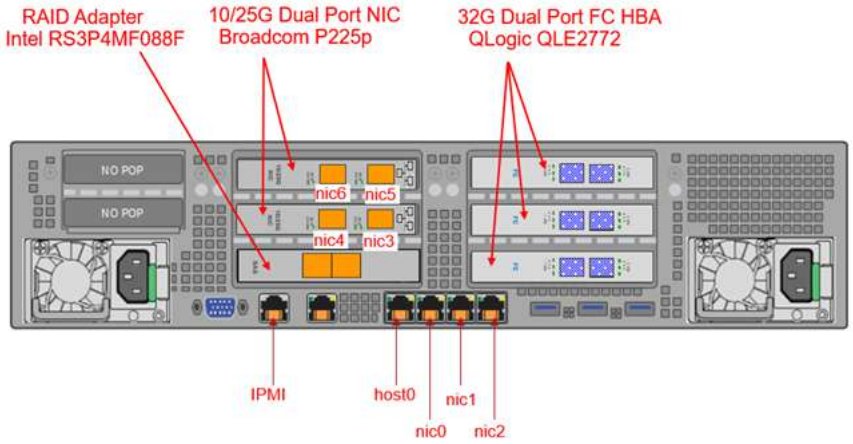
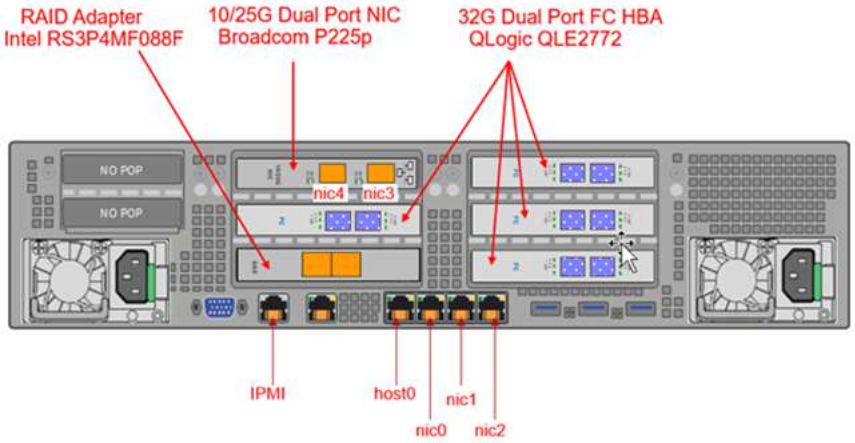


Figure 1-10 Flex 5260 Model D



Veritas 5260 Appliance total I/O on-board and PCIe ports

Table 1-10 Total number of Veritas 5260 Appliance on-board and PCIe I/O ports for each I/O configuration

I/O Configuration option	10 GbT Ethernet ports (copper)	10/25 Gb Ethernet PCIe ports (optical/SFP)	32 Gb Fibre Channel PCIe ports (optical/SFP)
A	4 on-board	2	2
B	4 on-board	6	4
C	4 on-board	4	6
D	4 on-board	2	8

Cable connection types:

copper = Standard copper cable

optical = Fiber optic cable

Customizable I/O configurations by slot for existing Veritas 5260 Appliance

You can use the supported Veritas 5260 Appliance I/O configurations to best serve the needs of your particular environment.

The controller is installed in both non-shelf and with-shelf configurations

The following table provides information on the make and model of each the PCIe cards that are available for use in each appliance I/O slot.

Table 1-11 Acceptable PCIe-based I/O cards for each appliance I/O slot

Slot	Acceptable PCIe I/O card	Comment
1	INTEL RS3P4MF088F 12Gb/s 8 port Internal / 8 port External PCI-Express 4.0 X 8 SAS RAID controller	External RAID controller to which you connect a Veritas 2U12 65.5TiB/72TB Storage Shelf
2	QLE2772 dual-port 32 Gb Fibre Channel host bus adapter Broadcom P225p Ethernet card	PCIe-based 32 Gb Fibre Channel host bus adapter PCIe-based 10/25 Gb network interface card
3	Broadcom P225p Ethernet card	PCIe-based 10/25 Gb network interface cards
4	QLE2772 dual-port 32 Gb Fibre Channel host bus adapter Broadcom P225p Ethernet card	PCIe-based 32 Gb Fibre Channel host bus adapter PCIe-based 10/25 Gb network interface cards
5	QLE2772 dual-port 32 Gb Fibre Channel host bus adapter	PCIe-based 32 Gb Fibre Channel host bus adapter
6	QLE2772 dual-port 32 Gb Fibre Channel host bus adapter	PCIe-based 32 Gb Fibre Channel host bus adapter

Broadcom P225p 10/25Gb PCIe Ethernet card

The Broadcom® BCM957414A4142CC is a dual-port 25 Gb/s, PCI-Express Gen3 x8 Network Interface Card that supports both SFP28/SFP+ optical modules and copper direct attach cable. The card uses the Broadcom BCM57414 25GbE MAC controller with the integrated dual channel 25GbE SFI transceiver.

By default, a 10 GB SFP is shipped with the appliance.

Note: Veritas recommends that you use Finisar FTLX8574D3BCV SFP part for 10G connectivity and Broadcom AFBR-735SMZ SFP part for 25G connectivity.

Table 1-12 Broadcom P225p NIC adapter specifications

Item	Specification
Bracket height	Full height
Power consumption	Typical: 12.5 watts Maximum: 12.9 watts
Operating temperature	0°C to 55°C (32 F to 131 F)
Storage temperature	-40°C to +70°C (-49°F to +221°F)
Storage humidity	90% at 35°C
System interface type	PCIe v3.0
Speed and slot width	8.0 GT/s (gigatransfers per second), 8-Lane
Data rate supported per port	10/25Gb
Air Flow (minimum)	150 LFM (linear feet per minute)

QLE2772 dual-port 32 Gb Fibre Channel host bus adapter

The QLE2772 dual-port 32 Gb Fibre Channel (FC) host bus adapter connects the appliance compute node to the storage area network.

Table 1-13 QLE2772 dual-port 32Gb Fibre Channel host bus adapter specifications

Item	Description
Bracket height	Full Height
Form factor	Low-profile PCIe card (6.6 inches × 2.731 inches)
Power consumption (watts)	Nominal: 11.0 W Maximum: 13.7 W
Operating temperature	0°C to 55°C (32°F to 131°F)
Storage temperature	–20°C to 70°C (–4°F to 158°F)
Operating humidity	10% to 90%
Storage humidity	5% to 95%

Table 1-13 QLE2772 dual-port 32Gb Fibre Channel host bus adapter specifications *(continued)*

Item	Description				
System interface type	PCIe v4.0				
Certifications	UL, CSA, TUV, CB, FCC, VCCI				
Maximum cable distances	**Rate**	**Cable and Distance (m)** (multimode optic cable)			
		OM2	**OM3**	**OM4**	**OM5**
	8 Gbps	50	150	190	190
	16 Gbps	35	100	125	125
	32 Gbps	20	70	100	100

Intel RAID Adapter RS3P4MF088F

The Intel RAID Adapter RS3P4MF088F is a tri-mode RAID Adapter with 12Gb SAS-3 MegaRAID 8 internal ports.

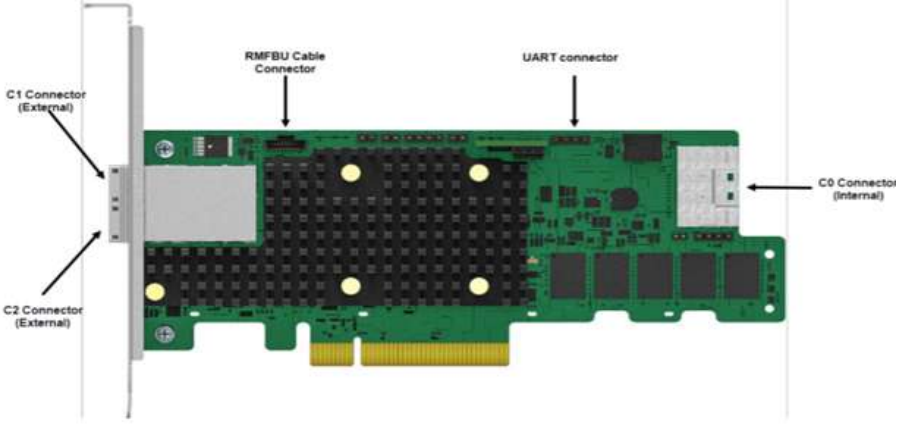


Table 1-14 RS3P4MF088F RAID adapter specifications

Item	Specification
Bracket height	Low profile mounting bracket
Power consumption	Typical: 16.70 watts Maximum: 17.71 watts
Operating temperature	0°C to 55°C (32 F to 131 F)
Storage temperature	-45°C to +105°C (-49°F to +221°F)
Storage humidity	20-80% RH (operating) 05-90% RH (non-operating)
System interface type	PCIe v4.0 (x8 PCI Express* 4.0 PCIe*)
Speed and slot width	16 GT/s (gigatransfers per second), per lane
Data rate supported per port	12, 6, 3 Gbps per port SAS 6, 3 Gbps per port SATA 16 Gbps per lane NVMe*
Air Flow (minimum)	200 LFM (linear feet per minute)

Chapter 2

Veritas 2U12 65.5TiB/72TB Storage Shelf

This chapter includes the following topics:

- Storage Shelf overview
- Usable appliance storage capacities
- Components of the Storage Shelf

Storage Shelf overview

Figure 2-1 5260 Appliance Storage Shelves

The optional Veritas 2U12 65.5TiB/72TB Storage Shelf is a 2U12 drive enclosure that contains twelve 8TB 7200 rpm SAS hard disk drives. Available storage capacity of the storage shelf is 65 TiB. Each disk drive can be accessed from the storage shelf's front panel. The PCIe RAID controller is used to configure the disk drives

into a RAID 6 configuration. One of the disk drives is reserved as a global hot spare and can be used in case of any drive failure.

The Storage Shelf also contains two Storage Bay Bridge 2.1 compliant (SBB) Input/Output (I/O) modules. Each I/O module has three mini-SAS HD ports, which are labeled A, B, and C. As such, each storage shelf contains a total of six mini-SAS HD I/O ports. However, only ports A and B of each I/O module are used to connect the storage shelf to the appliance or other storage shelves.

Each I/O module also includes one Ethernet port and a 3.5mm RS232 Interface-to-Enclosure Services Processor jack. The Ethernet port and the RS232 jack are only used during on-site debugging operations. They are not used during normal appliance operations.

Along with the I/O modules and the disk drives, the Storage Shelf also includes a front control panel. The control panel provides LED indications of the health of the storage shelf. It uses a dual seven segment display for enclosure identification and a switch that is used for storage shelf configuration purposes.

The Storage Shelf serial number appears on a plastic panel on the left side of Power Cooling Module 0 (PCM 0). The storage shelf serial number begins with the letters SH.

See "Storage Shelf front panel components" on page 33.

See "Storage Shelf rear components" on page 38.

See "Storage Shelf control panel" on page 35.

Usable appliance storage capacities

Table 2-1 Usable storage capacities - Veritas 5260 Appliance and Veritas 2U12 65.5TiB/72TB Storage Shelves

Appliance only	Storage shelf capacity	Appliance and one storage shelf	Appliance and two storage shelves	Appliance and three storage shelves	Appliance and four storage shelves	Appliance and five storage shelves	Appliance and six storage shelves
10TB (9.1TiB)	72TB (65.5TiB)	82TB (74.6 TiB)	154TB (140.1 TiB)	226TB (205.6 TiB)	298TB (271.1TiB)	370TB (336.6TiB)	442TB (402.1TiB)
40TB* (36.4TiB)	72TB (65.5TiB)	112TB (101.9TiB)	184TB (167.4TiB)	256TB (232.9TiB)	328TB (292.4TiB)	400TB 363.9TiB)	472TB (429.4TiB)

Note: Usable storage capacities are rounded values. Veritas calculates these values from the raw storage capacities of the various Veritas 5260 Appliance-only configurations. The raw capacity of the Veritas 2U12 65.5TiB/72TB Storage Shelf is 65.5 tebibyte. To determine the exact usable capacities of each configuration, use the following formulas: <appliance-only capacity> + 65.5 = exact usable capacity

* You can add up to six Storage Shelves to an existing Veritas 5260 Appliance with internal storage capacities of 9.1TiB or 36.4TiB. However, before you place the system into a production environment, you must migrate all MSDP data from the appliance to the first external storage shelf. After you migrate the MSDP data, the system's usable storage space may fluctuate, depending on how much actual storage space the MSDP data pool uses.

A 256GB memory upgrade kit is available for purchase when adding the first 2U12 65.5TiB/72TB Storage Shelf, which replaces all existing DIMM modules in the appliance. Contact your Veritas account representative for details.

Note: Spanning MSDP data across both Veritas 5260 Appliance internal storage and a storage shelf is not recommended as it may result in degraded performance.

Warning: Failure to migrate MSDP data after you connect a storage shelf may result in degraded appliance throughput performance.

For more information about migrating MSDP data, see the following document: Moving the MSDP partition from a base disk to an expansion disk for optimum performance.

Components of the Storage Shelf

The following sections describe the components of the Veritas 2U12 65.5TiB/72TB Storage Shelf.

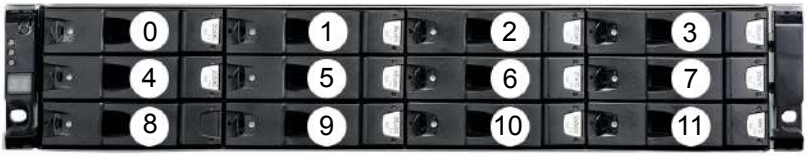
Storage Shelf front panel components

Hard disk drive capacities and drive bay slot assignments

The Veritas 2U12 65.5TiB/72TB Storage Shelf contains 12 disk drive storage bays that are populated with 8 TB 7200 rpm SAS hard disk drives. The available backup storage capacity of the storage shelf equals 65 TiB. One of the disk drives is reserved as a hot spare. All disk drives are accessible from the front panel of the storage shelf after you remove the storage shelf bezel.

The following figure shows the front panel disk drive slot assignments within the Veritas 2U12 65.5TiB/72TB Storage Shelf.

Figure 2-2 Veritas 2U12 65.5TiB/72TB Storage Shelf disk drive slot layout

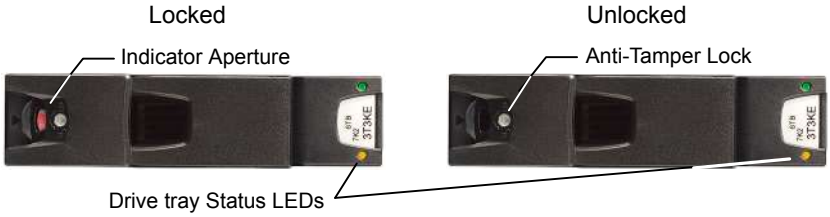


The storage shelf uses the drive that is located in slot 11 as a hot-spare drive.

Hard disk drive carrier characteristics

Each storage shelf hard drive is housed in a disk drive carrier. Each disk drive carrier uses a locking mechanism that secures the disk drive within the storage shelf.

Figure 2-3 Hard disk drive tray components



The following table describes the disk drive carrier LEDs. Note that the combination of both LEDs provides the status.

Table 2-2 Veritas 2U12 65.5TiB/72TB Storage Shelf disk drive carrier LED status

Status	Activity (green) LED	Fault (amber) LED
No disk drive installed.	OFF	OFF
Drives are installed, turned on, and operational.	Blinks during I/O activity and during startup.	OFF
SCSI Enclosure Services (SES) Device identity set.	ON	Blinks at a rate of 1 second ON and 1 second OFF.
Drive slot fault.	OFF	ON

Table 2-2 Veritas 2U12 65.5TiB/72TB Storage Shelf disk drive carrier LED status *(continued)*

Status	Activity (green) LED	Fault (amber) LED
Drive fault. Power control circuit fault.	ON	ON
Logical fault. Possible drive failed.	ON	Blinks at a rate of 3 seconds ON and one 1 second OFF.

Note: For security purposes, each drive tray is locked by default when the storage shelf is shipped from the factory. To access a hard disk drive, each storage bay must be unlocked using a T10 torx screw driver.

Storage Shelf control panel

The Veritas 2U12 65.5TiB/72TB Storage Shelf control panel is installed on the front left side of the storage shelf.

Figure 2-4 Veritas 2U12 65.5TiB/72TB Storage Shelf control panel

Table 2-3 Veritas 2U12 65.5TiB/72TB Storage Shelf control panel functions

Number	Item	Description
1	Input switch	The Input switch enables you to set the Unit Identification display.
2	Power On / Standby LED (Green or Amber)	The Power On/Standby LED shows Amber when only standby power is available. Otherwise, the LED shows Green when system power is available.
3	Module Fault LED (Power Cooling Module, Cooling, I/O module status) (Amber)	The Module Fault LED illuminates when there is a system hardware fault. The system hardware fault may be associated with a fault LED on a Power Cooling Module (PCM) or on an I/O module.
4	Logical status LED (amber)	The Logical Status LED shows a change of status or a fault. Typically these changes of status or faults are associated with the shelf's disk drives. However, the Logical Status LED can also indicate an issue with an internal RAID controller or external RAID controller, or with a host bus adapter.

Table 2-3 Veritas 2U12 65.5TiB/72TB Storage Shelf control panel functions *(continued)*

Number	Item	Description
5	Unit Identification Display	The Unit Identification Display is a dual digit display that provides information about the storage shelf. Its primary function is to assist in the configuration of multiple storage shelves.

Table 2-4 Control panel LED conditions and statuses

System Power (Green or Amber)	Module Fault (Amber)	Logical Fault (Amber)	Associated LEDs/Alarms	Status
On (Amber)	Off	Off	None	Standby power present, Overall Power failed or switched off
On (Green)	On (Amber)	N/A	Single beep, then double beep	Control Panel Power on - test state (Test state = 5 seconds)
On (Green)	Off	Off	None	Power On - All functions good
On (Green)	On (Amber)	N/A	Power Cooling Module Fault LEDs Fan Fault LEDs	Any Power Cooling Module Fault, Fan Fault, or an over or under temperature issue
On (Green)	On (Amber)	N/A	I/O module LEDs	Any I/O module fault
On (Green)	On (Amber)	N/A	None	Enclosure Logical Fault
On (Green)	Flashing	N/A	Module Fault LED on an I/O module	Unknown I/O module type installed (Invalid or Mixed)
On (Green)	Flashing	N/A	Power Cooling Module Fault LEDs Fan Fault LEDs	Unknown Power Cooling Module installed. (Invalid or Mixed)

Table 2-4 Control panel LED conditions and statuses *(continued)*

System Power (Green or Amber)	Module Fault (Amber)	Logical Fault (Amber)	Associated LEDs/Alarms	Status
On (Green)	N/A	On	Array in a failed or degraded state	Drive failure has occurred causing loss of availability or redundancy
On (Green)	N/A	Flashing	Arrays in an impacted state	Array operating background function
On	Flashing	N/A	SES state S1	Enclosure ID setting different from "start of day" setting

N/A - Not Applicable

For more information, see the *Veritas 5260 Appliance Hardware Installation Guide*.

Storage Shelf rear components

This section describes the rear panel features of the Veritas 2U12 65.5TiB/72TB Storage Shelf.

The following figure provides an overview of the components that comprise the Veritas 2U12 65.5TiB/72TB Storage Shelf rear panel.

Figure 2-5 Veritas 2U12 65.5TiB/72TB Storage Shelf rear components

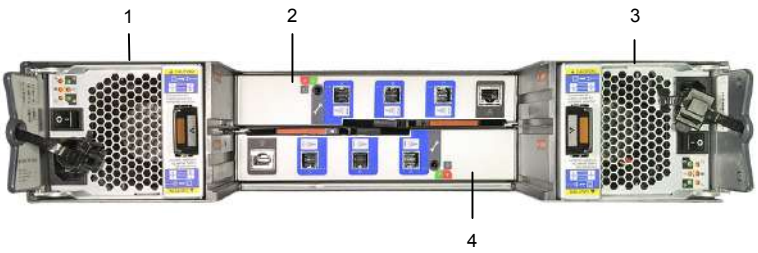


Table 2-5 Veritas 2U12 65.5TiB/72TB Storage Shelf rear components

Number	Component
1	Power Cooling Module 0 (PCM0)

Table 2-5 Veritas 2U12 65.5TiB/72TB Storage Shelf rear components *(continued)*

Number	Component
2	I/O module 0
3	Power Cooling Module 1 (PCM1)
4	I/O module 1

Storage Shelf I/O modules

This section discusses the Veritas 2U12 65.5TiB/72TB Storage Shelf I/O modules.

Figure 2-6 Veritas U12 65.5TiB/72TB Storage Shelf I/O module

The following figure and table provides details of the two Veritas 2U12 65.5TiB/72TB Storage Shelf I/O module canisters.

Figure 2-7 Veritas 2U12 65.5TiB/72TB Storage Shelf I/O modules

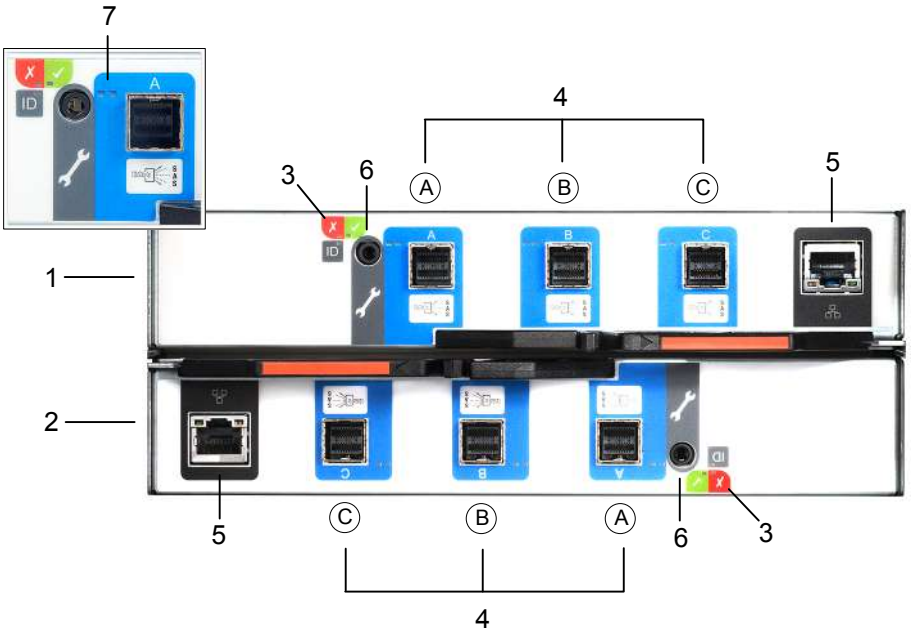


Table 2-6 Veritas 2U12 65.5TiB/72TB Storage Shelf I/O module components

Number	Description
1	I/O module 0
2	I/O module 1
3	I/O module Status LEDs See "I/O module Status LED location and conditions" on page 41.
4	mini-SAS HD ports - A, B, and C
5	Ethernet port (debugging purposes only)
6	RS232 jack (debugging purposes only)
7	SAS Activity LEDs See "I/O module SAS Activity LED location and conditions" on page 41.

I/O module Status LED location and conditions

This section discusses the location of the Status LEDs on the I/O module and the Status LED conditions.

Figure 2-8 I/O module Status indicator LED location

Table 2-7 I/O module Status LED conditions

Condition	Activity LED (green)	Fault LED (amber)
Module Fault (amber)	On	The I/O module has encountered a fault condition.
	Off	The I/O module is operating normally.
Power (green)	On	The I/O module is on.
	Off	The I/O module is off.
ID (blue)	On	The I/O module controller is being identified.

I/O module SAS Activity LED location and conditions

This section discusses the location of the SAS Activity LEDs on the I/O module and the SAS Activity LED conditions.

Figure 2-9 I/O module SAS Activity LED location

Table 2-8 I/O module SAS Activity LED conditions

Condition	Activity LED (green)	Fault LED (amber)
No Cable Present	Off	Off
Cable Present All links up, no activity.	On	Off
Cable Present All links up.	Flash with aggregate port activity	Off
Critical Fault Any fault which causes operation of the cable to cease or fail to start. For example, an OVERCURRENT trip.	Off	On
Non-Critical Fault Any fault which does not cause the connection to cease operation. For example, not all links established; OVERTEMPERATURE condition detected.	Flash with aggregate port activity	Flashing - One second on; one second off

Storage Shelf Power Cooling Modules

The Veritas 2U12 65.5TiB/72TB Storage Shelf includes two Power Cooling Modules (PCM). The dual PCMs provide redundant power to the storage shelf. If one PCM fails, the storage shelf continues to operate as the second PCM continues to supply the storage shelf with power.

Figure 2-10 Power Cooling Module

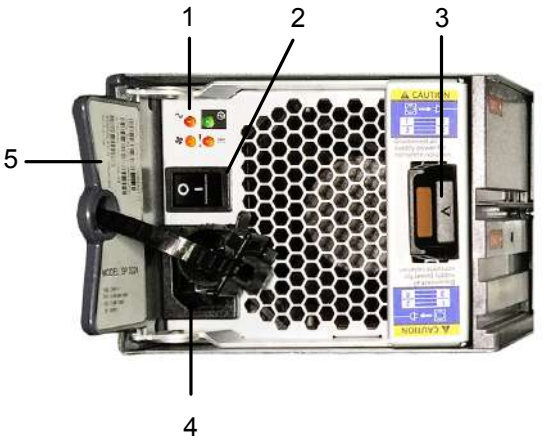


Table 2-9 Power Cooling Module components

Number	Component
1	Power Cooling Module LEDs See "Power Cooling Module LEDs" on page 44.
2	On/Off switch
3	Release tab
4	AC power socket

Table 2-9 Power Cooling Module components *(continued)*

Number	Component
5	Serial number - located on the Power Cooling Module 0 tab **Note:** The storage shelf serial number begins with the letters **SH**. 

Power Cooling Module LEDs

The Power Cooling Modules (PCM) use four LEDs to indicate the status of the PCM.

Figure 2-11 Power Cooling Module LEDs

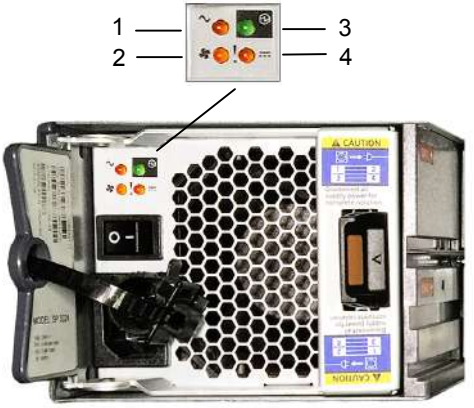


Table 2-10 Power Cooling Module LED legend

Number	LED condition
1	AC fail
2	Fan fail
3	Power Cooling Module OK
4	DC fail

Table 2-11 Power Cooling Module LED conditions

Status	Power Cooling Module OK (Green)	Fan Fail (Amber)	AC Fail (Amber)	DC Fail (Amber)
No AC Power (any Power Cooling Module)	Off	Off	Off	Off
No AC Power (this Power Cooling Module only)	Off	Off	On	On
AC Present (Power Cooling Module On OK)	On	Off	Off	Off
Power Cooling Module fan out of tolerance	On	Off	Off	On
Power Cooling Module fan fail	Off	On	Off	Off
Power Cooling Module Fault (Over temp, over volts, over current)	Off	On	On	On
Standby Mode	Flashing	Off	Off	Off
Power Cooling Module firmware download	Off	Flashing	Flashing	Flashing

See “Storage Shelf Power Cooling Modules” on page 42.

Chapter 3

Veritas 5260 Appliance and Veritas 2U12 65.5TiB/72TB Storage Shelf cables

This chapter includes the following topics:

- Power cables
- Network cable
- Multi-Mode fiber optic cable
- Twinaxial copper cables
- SAS-3 cable

Power cables

Power cables include a live line, a neutral line, and a grounding line.

Figure 3-1 AC power cable

A AC power connector (IEC-60320-C14) to an external power supply Power Distribution Unit (PDU) on a rack.

B AC power connector (IEC-60320-C13) to an appliance or a storage device.

Note: If your power distribution unit is not compatible with the IEC-60320-C14 plug, then Veritas recommends that you purchase your power cable locally. Make sure the power cable meets or exceeds the indicated power rating.

See "Multi-Mode fiber optic cable" on page 48.

See "SAS-3 cable" on page 50.

See "Twinaxial copper cables" on page 49.

See "Network cable" on page 47.

Network cable

The appliance communicates with the Ethernet networks through an Ethernet network cable. One end of the network cable connects to the management network port or service network port of the appliance. The other end of the cable connects to the network switch or an external gateway. Both ends of the cable are RJ45 connectors.

Figure 3-2 Network cable

See “Power cables” on page 46.

See “Multi-Mode fiber optic cable” on page 48.

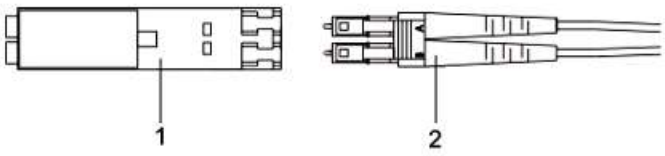
See “SAS-3 cable” on page 50.

See “Twinaxial copper cables” on page 49.

Multi-Mode fiber optic cable

Figure 3-3 Multi-Mode fiber cable

Fiber optic cables require Small Form-factor Pluggable (SFP+) transceivers, which are provided with each device having Fibre Channel ports. The diagram shows the SFP, labeled 1, and the fiber optic cable which is attached to it, labeled 2.



Supported SFPs are listed:

- Finisar
- JDSU

Note: Veritas recommends that you use Finisar FTLX8574D3BCV SFP part for 10G connectivity and Mellanox MMA2P00-AS SFP part for 25G connectivity.

See “Power cables” on page 46.

See “SAS-3 cable” on page 50.

See “Twinaxial copper cables” on page 49.

See “Network cable” on page 47.

Twinaxial copper cables

These cables are also known as Direct-Access Copper (DAC) cables, and are available in 1-meter, 3-meter, or 5-meter lengths.

See “Power cables” on page 46.

See “Multi-Mode fiber optic cable” on page 48.

See “SAS-3 cable” on page 50.

See “Network cable” on page 47.

SAS-3 cable

SAS-3 data cables are used to connect the optional Veritas 2U12 65.5TiB/72TB Storage Shelf to the Veritas 5260 Appliance. SAS-3 cables have a mini-SAS HD connector on both ends. Two 1m SAS-3 cables are shipped with each S Series Storage Shelf. For the D Series Storage Shelves, a 2 meter cable is standard. Longer SAS-3 cables are supported with the 2U12 Storage Shelf if needed for the configuration.

Figure 3-4 SAS-3 cable

See “Power cables” on page 46.

See “Multi-Mode fiber optic cable” on page 48.

See “Twinaxial copper cables” on page 49.

See “Network cable” on page 47.

Appendix A

Technical specifications, Environmental/Protocol standards, and Compliance standards

This appendix includes the following topics:

- Veritas 5260 Appliance technical specifications
- Veritas 2U12 65.5TiB/72TB Storage Shelf technical specifications
- Environmental specifications
- Protocol standards
- Regulatory, compliance, and certification information
- Product regulatory compliance
- Country approvals
- Product safety compliance
- Product EMC Compliance - Class A Compliance
- Product environmental compliance

Veritas 5260 Appliance technical specifications

The following table provides technical specifications for the Veritas 5260 Appliance.

Table A-1 Veritas 5260 Appliance technical specifications

Technical Specification	Veritas 5260 Appliance
Rack information	19" EIA standard The rack rails that are provided for the 5260 Appliance compute node are extensible to 32” (820mm). The minimum distance or depth allowed between the rack posts is 24.6” (623mm). The maximum distance or depth allowed between the rack posts is 37” (942mm). If the distance between rack posts is longer than 37” (942mm), the rails and the appliance cannot be properly installed.
Processor	Intel Xeon Scalable Third generation Silver 4314
CPU speed	2.40 GHz
Cores	32 (16 per processor)
System memory (currently supported)	64 GB 256 GB 512GB **Note:** When you purchase the first expansion storage shelf, the Storage Expansion Kit that comes with the storage shelf includes 256 GB of memory that replaces the existing 64GB. Additional 256GB memory kit is required when you add the fifth shelf.
Memory type and configuration (DIMMs)	DDR4 RDIMM 8 x 8GB (64GB) 8 x 32GB (256GB) 16 x 32GB (512GB)
SAS RAID card installed in a PCIe riser assembly (Y/N)	PCIe RAID card: Yes
RAID cache	4 GB is also included on the external PCIe RAID controller
Usable MSDP and AdvancedDisk storage capacity (TiB)	Appliance: 9.1TiB, 36.4TiB Each storage shelf: 65.5TiB Maximum configuration shipped from the factory: 429.4TiB
Maximum number of storage shelves	6

Table A-1 Veritas 5260 Appliance technical specifications *(continued)*

Technical Specification	Veritas 5260 Appliance
10 Gb Ethernet ports	Up to 4 maximum
10/25 Gb Ethernet ports	Up to 6 maximum
32 Gb Fibre Channel ports	Up to 8 maximum
Dimensions (IEC rack compliant)	Height: 8.9cm (3.5") (approximately 2U) Width: 43.9cm (17.28“) Depth: 71.2cm (28.03“)
Maximum weight	23.3 kg (51.37 lbs)
AC power requirements	110 VAC at 6.2 A 220 VAC at 3.2 A
AC power cable	Specification: IEC-60320-C14 to IEC-60320-C13, 10A/250V, Black, 4 ft The IEC-60320-C14 plugs into a Power Distribution Unit. The IEC-60320-C13 plugs into an appliance or storage shelf power supply. **Note:** If your power distribution unit is not compatible with the IEC-60320-C14 plug, then Veritas recommends that you purchase your power cable locally. Make sure the power cable meets or exceed the indicated power rating. See “Power cables” on page 46.
AC Frequency range	50/60Hz
Typical power consumption	400 watts
Typical power consumption with a maximum of six connected external storage shelves	1,936 watts
Maximum power consumption	1100 watts
Maximum power consumption with a maximum of six connected external storage shelves	3,980 watts

Table A-1 Veritas 5260 Appliance technical specifications *(continued)*

Technical Specification	Veritas 5260 Appliance
System cooling requirement (heat dissipation)	1365 BTU/hr (Typical) 3753 BTU/hr (Maximum)
System cooling requirement with maximum external storage (heat dissipation)	6606 BTU/hr (Typical) 13580 BTU/hr (Maximum)
Operating voltage	90V – 140 VAC 180V – 264 VAC
Power conversion efficiency	90% +
Acoustic noise	70 dBA

See "Veritas 2U12 65.5TiB/72TB Storage Shelf technical specifications" on page 55.

See "Environmental specifications" on page 57.

Veritas 2U12 65.5TiB/72TB Storage Shelf technical specifications

The following table provides technical specifications for a Veritas 2U12 65.5TiB/72TB Storage Shelf.

Table A-2 Veritas 2U12 65.5TiB/72TB Storage Shelf technical specifications

Technical specification	Description
Rack information	The rack installation height is the space occupied by a storage shelf in a rack cabinet. The height for the storage shelf is 3.5 inches, 88.9mm. The shelf fits into a 2U rack space. Install the storage shelf in a rack cabinet that is 19 inches (483mm) wide. The rack rails that are provided for the storage shelf are extensible to 32" (813mm). This distance is the maximum depth that is allowed between rack posts. If the distance between rack posts is longer than 32" (813mm) the rails and the appliance cannot be properly installed.
Hot swappable components	Disk drives, power cooling modules, and I/O modules (Storage Bay Bridge (SBB) 2.1)

Table A-2 Veritas 2U12 65.5TiB/72TB Storage Shelf technical specifications *(continued)*

Technical specification	Description
Usable storage capacity (TB)	65.5TiB/72TB
Maximum weight (fully populated)	28 kg (62 lbs)
Shipping weight	52 kg (115 lbs)
Dimensions	Height: 8.89cm (3.5") (approximately 2U) Width: 48.26cm (19") ICE rack compliant Depth: 60.20cm (23.7")
Device types supported	Dual ported 12Gb/s SAS drives
Maximum drives per enclosure	12
Typical power consumption	256 watts per storage shelf You can connect a maximum of six storage shelves to the Veritas 5260 Appliance.
Maximum power consumption	480 watts per storage shelf You can connect a maximum of six storage shelves to the Veritas 5260 Appliance.
System cooling requirement (heat dissipation)	873 BTU/hr (typical) 1637.8 BTU/hr (Maximum)
Operating voltage	100V - 127VAC 200V - 240VAC
AC Frequency range	50/60Hz
Power conversion efficiency	>80% @ 100V, >80% @240V (>30% load)
Acoustic noise	63 dBA
Non-operational altitude	-300 to 12,192 m (-1,000 to 40,000 ft)
Operational shock	2g 11mSec half sine
Non-operational shock	25g 10mSec half sine
Operational vibration	0.21g RMS 5-500Hz random
Non-operational vibration	1.04g RMS 2-200Hz random

Table A-2 Veritas 2U12 65.5TiB/72TB Storage Shelf technical specifications *(continued)*

Technical specification	Description
Relocation vibration (Non-operational)	0.3g 2-200Hz sinusoidal

See "Veritas 5260 Appliance technical specifications" on page 52.

See "Environmental specifications" on page 57.

Environmental specifications

Veritas Appliance compute node environmental specifications

Table A-3 Veritas Appliance compute node environmental specifications

Specification	5260 Appliance compute node
Operating temperature	ASHRAE A2 (10°C to 35°C) (50°F to 95°F)
Non-operating temperature	-40 °C to 70 °C (-40 °F to 158 °F) The non-operating temperature is defined as the temperature of the system when the system is turned off. It is also referred to as the storage temperature. Veritas recommends that you do not store the system in an environment where the temperatures fall outside of the listed temperature range.
Operating humidity (RH)	20% RH to 80% RH
Non-operating humidity	8% RH to 90% RH
Operating altitude (feet)	3050 m (10,006 ft)
Temperature gradient (per hour)	10°C/h (50°F/h)

See "Veritas 5260 Appliance technical specifications" on page 52.

See "Veritas 2U12 65.5TiB/72TB Storage Shelf technical specifications" on page 55.

See "Protocol standards" on page 58.

See "Regulatory, compliance, and certification information" on page 58.

Protocol standards

The following table provides standards with which the Veritas 5260 Appliance and the Veritas 2U12 Storage Shelf comply.

Table A-4 Veritas 5260 Appliance / Veritas 2U12 Storage Shelf standards compliance

Standard	Version
IPMI 2.0	Intelligent Platform Management Interface Specification Second Generation v2.0, Document Revision 1.0
SMBIOS	System Management BIOS (SMBIOS) Reference Specification, Version 3.5.0
SAS	SAS - 3.0
ACPI	Advanced Configuration and Power Interface Specification, Revision 6.3
IP	RFC0791: Internet Protocol
FC	INCITS T11 (X3T9.3)
PCIe Express	PCIe 4.0

See "Veritas 5260 Appliance technical specifications" on page 52.

See "Veritas 2U12 65.5TiB/72TB Storage Shelf technical specifications" on page 55.

See "Environmental specifications" on page 57.

Regulatory, compliance, and certification information

The following sections give information about the product regulations and compliance.

WARNING

To ensure regulatory compliance, you must adhere to the assembly instructions in this guide to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components that are specified in this guide. Use of other products or components may void the regulatory approvals of the product. The result is noncompliance with product regulations in the region in which the product is sold.

Alterations to the configuration of your appliance may require additional compliance testing.

This product is an FCC Class A device. Integration of it into a Class B system does not result in a Class B device.

Product regulatory compliance

The appliance, when correctly integrated per this guide, complies with the following safety and electromagnetic compatibility (EMC) regulations.

Intended Application - This product was evaluated as Information Technology Equipment (ITE), which may be installed in offices, schools, computer rooms, and similar commercial type locations. The suitability of this product for other product categories and environments, other than an ITE application, may require further evaluation. Other product categories and environments may include medical, industrial, telecommunications, NEBS, residential, alarm systems, and test equipment.

Country approvals

- US/Canada
- CE - European Union (EU)
- Australia / New Zealand
- KCC South Korea
- IRAM Certification (Argentina)
- CCC Certification (China)

- BIS India
- NOM Mexico
- InMetro Brazil
- NRCS & SABS South Africa
- BSMI Taiwan
- VCCI Japan

Note: Other countries are either based on these requirements or do not require certification. For more regulatory compliance information please refer to this link: Regulatory Compliance / Homologation

Product safety compliance

The following is a list of product safety compliance norms for different countries:

- EN 62368-1:2014 + AC:2015
- EU Directive: Low Voltage 2014/35/EU
- CSA C22.2 No. 62368-1
- CB Certificate & Report, IEC62368-1 (report to include all country deviations)

Product EMC Compliance - Class A Compliance

The following is a list of EMC compliance norms for different countries:

- EU Directive: EMC 2014/30/EU
- EN 55035:2017 +A11:2020
- EN 55032:2015 +A11:2020
- EN 61000-3-2:2014
- EN 61000-3-3:2013
- FCC /ICES-003 - Emissions (USA/Canada) Verification
- VCCI Emissions (Japan)
- AS/NZS 3548 Emissions (Australia / New Zealand)

Note: For a complete list of regulatory notices please refer to this link:

Veritas Safety and Compliance Guide

Product environmental compliance

Use of banned substances are restricted in accordance with world-wide regulatory requirements. Restrictions include quantity limitations on the following:

- Quantity limit of 0.1% by mass (1000 PPM) for: Lead, Mercury, Cadmium, Hexavalent Chromium, Polybrominated Biphenyls Diphenyl-Ethers (PBB/PBDE), Bis (2-ethylhexyl) phthalate (DEHP), Benzyl butyl phthalate (BBP), Dibutyl phthalate (DBP), Diisobutyl phthalate (DiBP).
- Quantity limit of 0.01% by mass (100 PPM) for: Cadmium
- California Code of Regulations, Title 22, Division 4.5, Chapter 33: Best Management Practices for Perchlorate Materials
- China - Restriction of Hazardous Substances (China RoHS)
- India RoHS
- EU WEEE Directive
- EU Packaging Directive
- EU Batteries Directive
- EU Commission Regulation (EU) 2019/424 of 15 March 2019
- EU REACH Regulation

Product environmental declarations of compliance are available in this link.

Index

A

Appliance
- configurations 6
- overview 6
- usable storage capacities 32

C

cables
- multi-mode fiber optic
  - description 48
- network
  - description 47
- power
  - description 46
- SAS-3
  - description 50
- Twinaxial copper
  - description 49

E

Environmental specifications 57

O

overview
- appliance 6

P

protocol standards
- Veritas 5260 Appliance / Veritas 2U12 Storage Shelf 58

U

usable storage capacities
- appliance 32

Veritas Access 3350 Appliance Product Description

VERITAS™

Veritas Access 3350 Appliance Product Description

Last updated: 2023-03-06

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://www.veritas.com/content/support/en_US/dpp.Appliances.html

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

APPL.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1 About the Access 3350 Appliance 6

About the Veritas Access 3350 Appliance 7
Features and components of the appliance 8
Locating the appliance serial number 12
About 3350 compute node disk drive configurations 13
About the compute node disk drive LEDs 14
About the compute node front panel USB port 15
About the compute node control panel 15
About the System Status LED states 17
About the Power button LED states 21
About the compute node rear panel 21
Standard 3350 Appliance PCIe-based I/O configuration 23
Total 3350 Appliance on-board and PCIe-based I/O ports 24
3350 Appliance network interface card port assignments 26
SAS3 host bus adapter connector locations and labels 27

Chapter 2 About the Veritas 5U84 Storage Shelves 30

About Veritas Access 3350 Appliance storage shelves 31
Available appliance storage options 33
About the Veritas 5U84 Storage Shelf disk drive drawers 35
5U84 Primary Storage Shelf and the 5U84 Expansion Storage Shelf control panel 47
About the 5U84 Primary Storage Shelf and 5U84 Expansion Storage Shelf rear components 48
Veritas 5U84 Primary Storage Shelf RAID controllers 51
Veritas 5U84 Expansion Storage Shelf Expansion I/O modules 55
Veritas 5U84 Storage Shelf cooling modules 58
5U84 Storage Shelf Power Supply Units 59

Chapter 3 Access 3350 Appliance and 5U84 Storage Shelf cables 61

Power cables 61
Network cable 64

Multi-mode fiber optic cable 64
SAS-3 cable 65
Twinaxial copper cables 67

Appendix A Technical specifications, Environmental/Protocol standards, and Compliance standards 68

3350 Appliance compute node technical specifications 69
Veritas 5U84 Storage Shelf technical specifications 72
Environmental specifications 75
Protocol standards 75
Regulatory, compliance, and certification information 76
Product regulatory compliance 77
Product safety compliance 77
Product EMC Compliance - Class A Compliance 77
Product ecology compliance 78
Certifications / Registrations / Declarations 78
Electromagnetic compatibility notices 79

Index 81

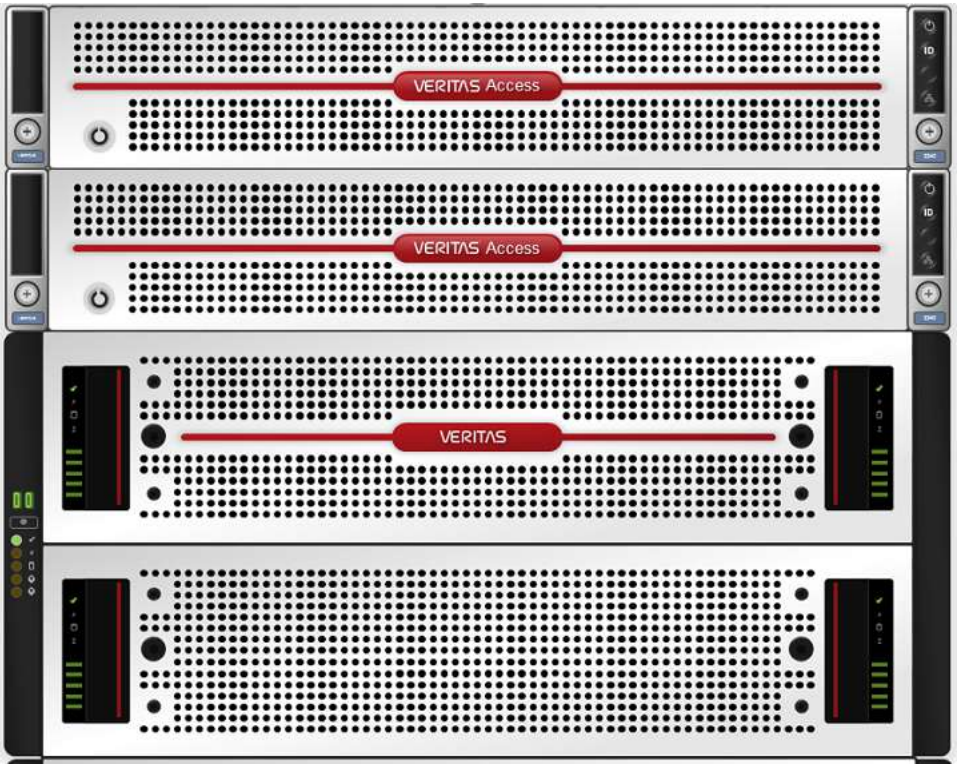
Chapter 1

About the Access 3350 Appliance

This chapter includes the following topics:

- About the Veritas Access 3350 Appliance
- Features and components of the appliance
- Locating the appliance serial number
- About 3350 compute node disk drive configurations
- About the compute node front panel USB port
- About the compute node control panel
- About the compute node rear panel
- Standard 3350 Appliance PCIe-based I/O configuration

About the Veritas Access 3350 Appliance



The Veritas Access 3350 Appliance is a highly available hardware and software storage system that can scale up to a total of 2544 TiB (2800 TB) of usable backup capacity depending on the storage configuration you purchase. It consists of two 2U 3350 Appliance compute nodes and at least one required externally attached 5U84 Primary Storage Shelf, which is used for data storage purposes. 3350 Appliance compute nodes do not provide internal disk space for data storage. You can add additional storage shelves if you require additional usable data storage space.

Note: Total usable backup capacity depends on the hardware configuration you purchase.

See “Available appliance storage options” on page 33.

SAS-3 cables connect the 3350 Appliance compute nodes to 5U84 Primary Storage Shelf RAID controllers. SAS-3 cables also connect 5U84 Primary Storage Shelves to the optional 5U84 Expansion Storage Shelves.

See See "About Veritas Access 3350 Appliance storage shelves" on page 31.

Features and components of the appliance

This section describes the features and components of the Veritas Access 3350 Appliance.

Table 1-1 Access 3350 Appliance system specifications

Technical Specification	Access 3350 Appliance system
Number of compute nodes per 3350 Appliance system	2
Processor model (each compute node)	■ Dual Intel® Xeon® Scalable Processors ■ Supports high-performance processors with low-power consumption ■ Provides high efficiency and performance
CPU speed	2.2 GHz (Turbo: 3.2 GHz)
Cores (each compute node)	20 (10 per processor)
Smart Cache (each compute node)	13.75 MB
System memory (per compute node)	Base memory capacity: 384GB Memory type: DDR4 LRDIMM Configuration: 6 x 64GB LRDIMM modules Operating voltage: 1.2V Configured clock speed: 2400MHz Maximum clock speed: up to 3200MHz
Usable AdvancedDisk storage capacity (TB)	Usable AdvancedDisk storage capacity: up to 2544 TiB (2800 TB) See "Available appliance storage options" on page 33.
SAS RAID mezzanine card	Yes

Table 1-1 Access 3350 Appliance system specifications *(continued)*

Technical Specification	Access 3350 Appliance system	
SAS RAID PCIe card installed in a appliance compute node PCIe riser assembly	No	
RAID levels	RAID1 (mirroring) and RAID6 (block level striping with double distributed parity) are used as follows: ■ RAID1: 3350 Appliance compute node system disks ■ RAID6: 5U84 Primary Storage Shelf and 5U84 Expansion Storage Shelf data storage disks **Note:** RAID levels are generated using an onboard Intel RMSHC080 RAID controller that is installed in each 3350 Appliance compute node.	
Maximum number of storage shelves	4 **Note:** Depending on the storage configuration purchased, the maximum number of storage shelves consists of one required 5U84 Primary Storage Shelves and up to three optional 5U84 Expansion Storage Shelves. See "Available appliance storage options" on page 33.	
I/O Ports See "Standard 3350 Appliance PCIe-based I/O configuration" on page 23. See "Total 3350 Appliance on-board and PCIe-based I/O ports" on page 24.	Two 12Gb SAS3 host bus adapters (PCIe-based)	Used to connect both of the Access 3350 Appliance compute nodes to the 5U84 Primary Storage Shelf
	10/25GB Ethernet PCIe-based network interface card	Two ports
	1Gb Ethernet ports	Four on-board ports
Rack information	19" EIA standard	

Table 1-1 Access 3350 Appliance system specifications *(continued)*

Technical Specification	Access 3350 Appliance system
Dimensions (IEC rack compliant)	**Each Appliance compute node** ■ Height: 8.89cm (3.5") (approximately 2U) ■ Width: 48.35cm (19") ■ Depth: 79.38cm (31.25") See " 3350 Appliance compute node technical specifications" on page 69. **5U84 Primary Storage Shelf / 5U84 Expansion Storage Shelf** ■ Height: 21.97cm (8.65") (approximately 5U - shelf, overall) ■ Width: 48.26cm (19") (across the mounting flange) ■ Length/depth: 93.35cm (36.75") (from rear of the front flanges to the rear extremity of the chassis) **Note:** The Veritas 5U84 Primary Storage Shelf and the 5U84 Expansion Storage Shelf are longer than what a standard IEC-compliant rack normally supports. Due to the additional length, the rack-based PDU hardware may need to be installed on the outside of the rack to accommodate the storage shelves. See " Veritas 5U84 Storage Shelf technical specifications" on page 72.
Maximum weight	Each Appliance compute node: 23.26 kg (51.28 lbs) 5U84 Primary Storage Shelf: 128 kg (282 lbs) with drives and rail kit 5U84 Expansion Storage Shelf: 128 kg (282 lbs) with drives and rail kit
Typical power consumption	**Each Appliance compute node** ■ 260 watts **Each storage shelf** ■ 1000 watts
Maximum power consumption	**Each Appliance compute node** ■ 500 watts **Each storage shelf** ■ 1300 watts

Table 1-1 Access 3350 Appliance system specifications *(continued)*

Technical Specification	Access 3350 Appliance system
Typical power consumption with a maximum of four external storage shelves	4,200 watts (two servers per cluster)
Maximum power consumption with a maximum of four external storage shelves	6,200 watts (two servers per cluster) (500 watts maximum per server)
AC power requirements	**Each compute node:** ■ 110 VAC - 220 VAC at 2.6 A **Each storage shelf:** ■ 200 - 240 VAC at 6.67 A
AC power cable	**Each compute node:** ■ Specification: IEC-60320-C14 to IEC-60320-C13, 15A/250V, Black, 4ft The IEC-60320-C14 plugs into a Power Distribution Unit. The IEC-60320-C13 plugs into an appliance or storage shelf power supply. **Note:** If your power distribution unit is not compatible with the IEC-60320-C14 plug, Veritas recommends that you purchase your power cable locally. Make sure the power cable meets the indicated power rating. See "Power cables" on page 61. **Storage shelf:** ■ Specification: IEC-60320-C20 to IEC-60320-C19, 20A/250V, Black, 4ft The IEC-60320-C20 plugs into a Power Distribution Unit (PDU) on a rack. The IEC-60320-C19 plugs into an appliance or a storage shelf power supply. **Note:** If your power distribution unit is not compatible with the IEC-60320-C20 plug, Veritas recommends that you purchase your power cable locally. Make sure the power cable meets the indicated power rating. See "Power cables" on page 61.

Table 1-1 Access 3350 Appliance system specifications *(continued)*

Technical Specification	Access 3350 Appliance system
Power Factor	> 90%
System cooling requirement (heat dissipation) (Appliance with maximum storage shelves attached)	**Typical** ■ 14,971 BTU/hour **Maximum** ■ 20,291 BTU/hour
Operating voltage	200 – 240 VAC
AC Frequency range	50/60 Hz
Power conversion efficiency	Each Appliance compute node: 90% + 5U84 Primary/Expansion Storage Shelf: 89% +
Acoustic noise	**Each Appliance compute node** ■ 70 dBA 5**U84 Primary/Expansion Storage Shelf** ■ Sound Power Operating ≤ 8.0 Bels LWAd @ 23°

Locating the appliance serial number

A vertical bar on the rear panel of the appliance compute node contains the serial number.

About 3350 compute node disk drive configurations

The Veritas Access 3350 Appliance compute node contains three 2 TB SAS hard disk drives. Each disk drive is accessible from the compute node's front panel. An embedded RAID controller on the compute node's mainboard configures two of the three disk drives into a mirrored RAID1 volume.

The RAID1 volume is labeled Volume 0. The disk drives that are located in slot 0 and slot 1 are configured as the RAID1, VOLUME0 device. These disk drives contain the appliance operating system, the operating system swap file, and the Veritas Access application. You can hot-swap one of these disk drives at a time if a drive becomes problematic. However, you cannot operate the appliance if both disk drives are removed.

The appliance uses the disk drive that is located in slot 2 as a hot-spare disk. If a disk drive in RAID Volume0 experiences a hardware error, the appliance automatically initiates a RAID rebuild operation. During the rebuild operation, the appliance dynamically accesses the hot-spare disk from slot 2 and uses it to rebuild the RAID volume.

Figure 1-1 Veritas Access 3350 Appliance compute node front panel disk slot assignments

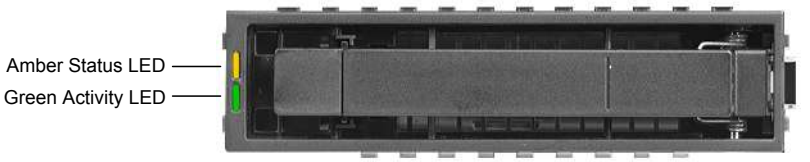
Table 1-2 Veritas Access 3350 Appliance compute node front panel disk drive configurations

Slot	RAID level	Disk drive size (TB)	Disk drive role
0, 1	RAID1	2 TB	Appliance operating system boot volume / operating system swap file / Veritas Access application
2		2 TB	Hot spare
3 - 11	No disk drives installed		

About the compute node disk drive LEDs

Each 3350 Appliance compute node disk drive module contains two LEDs on the left side of each module.

Figure 1-2 3350 Appliance compute node disk drive module LEDs



The LED Status descriptions are described in the following table.

Table 1-3 3350 Appliance compute node disk drive LED Status descriptions

Number	Description	LED behavior	Condition
1	Amber Status LED	Off	No disk drive access and no disk drive faults
		Solid amber	A disk drive fault has occurred
		Blinking amber	A RAID rebuild is in progress (1Hz blink) Locating / identifying the disk drive (4Hz blink)
2	Green Activity LED	Off	Power on - the disk drive has spun down
		Solid green	Power on - no disk drive activity
		Blinking green	Power on - the disk drive is processing a command or Power on - the disk drive is spinning up

Note: Disk drive modules that do not contain disk drives also have LEDs. Although there may not be disk drive activity, some colored lights may still be seen through the disk modules.

About the compute node front panel USB port

The 3350 Appliance compute node front panel includes a USB 2.0-compliant port that supports a data transfer rate of up to 480 Mb/second.

About the compute node control panel

The 3350 Appliance compute node includes a control panel on the right side of the front panel. System information is shown on this control panel.

Figure 1-3 Control panel

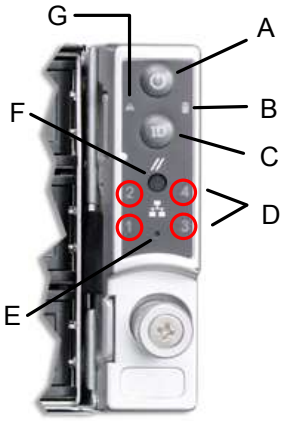


Table 1-4 Control panel system LED descriptions

Label	LED	System information
A	Power button with integrated LED	The Power button toggles the system on and off. See "About the Power button LED states" on page 21.
C	System ID button with integrated LED	The System ID button toggles the integrated ID LED and the blue server board LED on and off. The system ID LED identifies the system for maintenance when it is racked with similar server systems.
D	Network Activity LEDs	The front control panel includes four activity LED indicators for each on-board network interface controller (NIC). ■ NIC-1 represents network interface controller 1 ■ NIC-2 represents network interface controller 2 When network links are detected on the controllers, the LEDs are activated and remain on. The LEDs blink when network activity occurs, and the rate at which they blink is determined by the amount of network activity that occurs.
E	NMI button (recessed, tool required for use)	When it is depressed, the NMI button puts the appliance in a halt state, issues a non-maskable interrupt (NMI), and then triggers the non-maskable interrupt. All server data can be lost. Veritas recommends that you do not enable NMI by pressing the NMI button.
F	System Cold Reset Button (recessed, tool required for use on non-storage models)	When depressed, the System Cold Reset button re-boots and re-initializes the appliance.

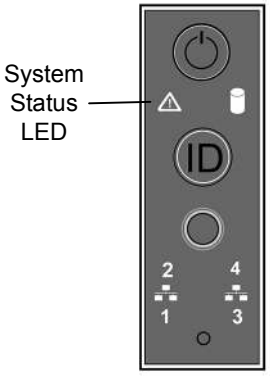
Table 1-4 Control panel system LED descriptions *(continued)*

Label	LED	System information
G	System Status LED	The System Status LED is bi-color indicator that uses the colors green and amber to display the current health of the appliance. Two locations are provided for you to monitor the health of the system. You can find the first location on the front control panel, while the second location is located on the back edge of the server board. It is viewable from the rear of the appliance. Both LEDs show the same state of health. See "About the System Status LED states" on page 17.

About the System Status LED states

The System Status LED is a bi-color (Green/Amber) indicator that shows the current health of the system. The appliance provides two locations for this feature. The first location is on the Front Control Panel, while the second location is on the back edge of the server board.

Figure 1-4 System Status LED control panel location



The following table provides a description of each LED state.

Table 1-5 System Status LED states

Color	State	Criticality	Description
No color	Off - The system is not operating.	Not ready	■ System power is off (AC and/or DC) ■ System is in EuP Lot6 Off Mode ■ System is in S5 Soft-Off State
Green	Solid on (SO)	Healthy	Indicates that the system is running (in S0 State) and its status is “Healthy”. The system is not exhibiting any errors. AC power is present and BMC has booted and manageability functionality is up and running.
Green	~1 Hz blink	Degraded The system is operating in a degraded state although still functional. or The system is operating in a redundant state but with an impending failure warning.	System degraded: ■ Redundant loss, such as power supply or fan. Applies only if the associated platform sub-system has redundancy capabilities. ■ Fan warning or failure when the number of fully operational fans is more than minimum number needed to cool the system. ■ Non-critical threshold crossed: Temperature (including HSBP temp), voltage, input power to power supply, output current for main power rail from power supply and Processor Thermal Control (Therm Ctrl) sensors. ■ Power supply predictive failure occurred while redundant power supply configuration was present. ■ Unable to use all of the installed memory (one or more DIMMs failed/disabled but functional memory remains available). ■ Battery failure ■ BMC executing in uBoot. (Indicated by Chassis ID blinking at 3Hz). System in degraded state (no manageability). BMC uBoot is running but has not transferred control to the BMC Linux. Server will be in this state 6-8 seconds after BMC reset while it pulls the Linux image into flash.

Table 1-5 System Status LED states *(continued)*

Color	State	Criticality	Description
Green	~1 Hz blink	Degraded (continued)	System degraded (continued): ■ BMC booting Linux. (Indicated by Chassis ID solid ON). System in degraded state (no manageability). Control has been passed from BMC uBoot to BMC Linux itself. It will be in this state for 10-20 seconds. ■ BMC Watchdog has reset the BMC. ■ Power unit sensor offset for configuration error is asserted. ■ Hard disk drive HSC is off-line or degraded.
Amber	~1 Hz blink	Non-critical The system is operating in a degraded state with an impending failure warning. However, the system is still functioning.	Non-fatal, although the system is likely to fail due to the following issues: ■ Critical threshold crossed – Voltage, temperature (including HSBP temp), input power to power supply, output current for main power rail from power supply and PROCHOT (Therm Ctrl) sensors. ■ VRD Hot asserted ■ Minimum number of fans to cool the system not present or failed ■ Hard drive fault ■ Power Unit Redundancy sensor – Insufficient resources offset (indicates not enough power supplies present) ■ Correctable memory error threshold has been reached for a failing DIMM when the system is operating in a non-redundant mode.

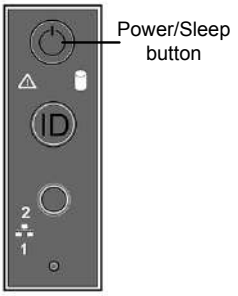
Table 1-5 System Status LED states *(continued)*

Color	State	Criticality	Description
Amber	Solid on	Critical, non-recoverable – System is halted	Fatal alarm – system has failed or shutdown: ■ CPU CATERR signal asserted ■ MSID mismatch detected (CATERR also asserts for this case) ■ CPU1 is missing ■ CPU Thermal Trip ■ No power – power fault ■ DIMM failure when there is only one DIMM present; no other good DIMM memory present ■ Runtime memory uncorrectable error in non-redundant mode.

Amber	Solid on	Critical, non-recoverable – System is halted	■ Uncorrectable Runtime memory error in non-redundant mode
			■ DIMM Thermal Trip or equivalent
			■ CPU ERR2 signal is asserted
			■ BMC/Video memory test failed (Chassis ID shows blue/solid-on for this condition)
			■ SBB Thermal Trip or equivalent
			■ 240VA fault
			■ Both uBoot BMC FW images are bad (Chassis ID shows blue/solid-on for this condition)
			■ Fatal Error in processor initialization:
			  ■ Processor family not identical
			  ■ Processor model not identical
			  ■ Processor core/thread counts not identical
			  ■ Processor cache size not identical
			  ■ Unable to synchronize processor frequency
			  ■ Unable to synchronize QPI link frequency

About the Power button LED states

Figure 1-5 Power button control panel location



About the compute node rear panel

The rear panel of the appliance compute node has several access ports and other features, which are displayed in the following figures.

Figure 1-6 Veritas 3350 Appliance compute node rear panel overview

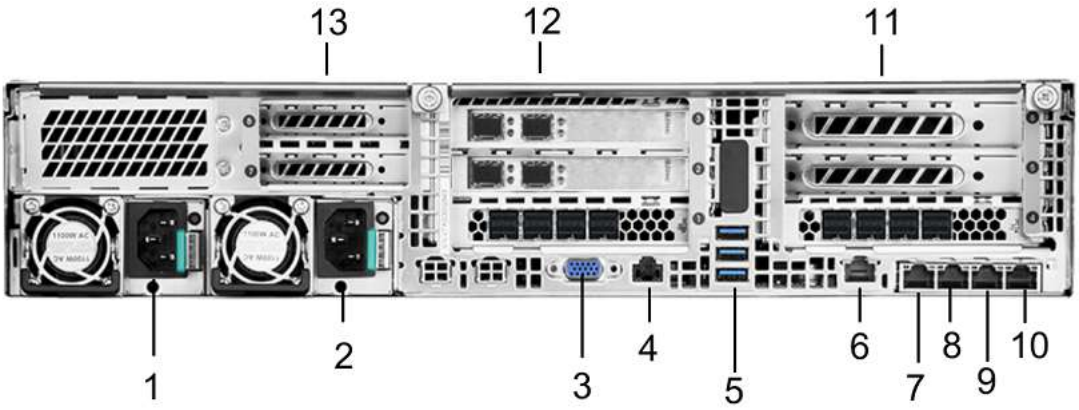


Table 1-6 Compute node rear panel features and connectors

Number	Function
1,2	Power Supply 1 and Power Supply 2 - Dual, redundant, and hot-swappable power supply modules
3	DB-15 VGA monitor connector

Table 1-6 Compute node rear panel features and connectors *(continued)*

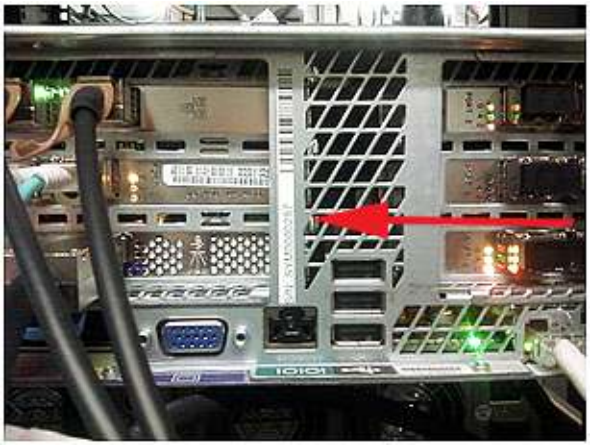
Number	Function
4	Serial port - Serial connection for Veritas Technical Support use only
5	Three stacked USB 3.0 Type A serial ports for general use
6	IPMI port - An external RJ45 port used for appliance remote management purposes
7	eth0/NIC1 A 1-GbE port copper connector that is reserved for use during the initial configuration of the 3350 Appliance **Note:** Veritas does not support forming a NIC bond using eth0/NIC1 with other eth/NIC ports.
8	eth1/NIC2
9	eth2/NIC3 A 1-GbE port copper connector The eth2 ports on each of the 3350 Appliance compute nodes attach to each other using straight through or cross-over cables. For example, eth2 on first compute node connects to eth2 of the second compute node.
10	eth3/NIC4 A 1-GbE port copper connector The eth3 ports on each of the 3350 Appliance compute nodes attach to each other using straight through or cross-over cables. For example, eth3 on first compute node connects to eth3 of the second compute node.
11	PCIe riser assembly 1
12	PCIe riser assembly 2
13	PCIe riser assembly 3 * (empty)

* 3350 Appliance compute nodes do not contain PCIe riser cards in PCI riser assembly 3.

Veritas appliances may include grounding studs in case your lab environment has such a requirement. The studs are located on the rear panel of the appliance. You can use standard grounding practices to connect grounding wires to the studs.

The serial number is located on a vertical bar on the rear panel of the appliance.

Figure 1-7 Serial number location



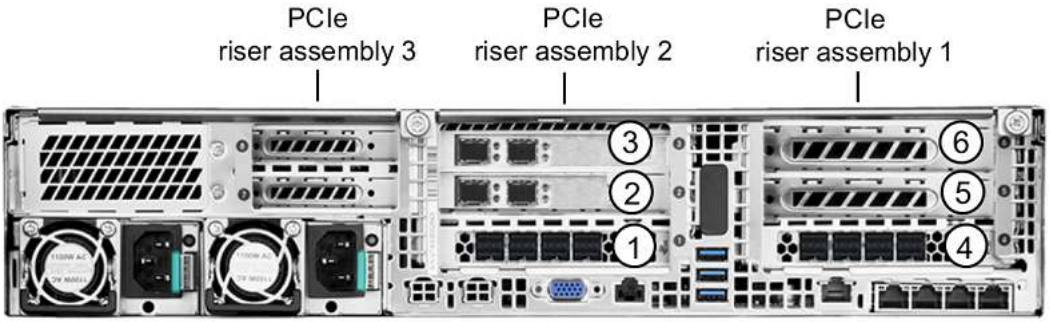
The ports on the rear panel are color-coded for easy identification.

Figure 1-8 Appliance rear port color codes

Standard 3350 Appliance PCIe-based I/O configuration

The rear panel of the Veritas Access 3350 Appliance contains three PCIe riser card assemblies. PCIe riser card assemblies 1 and 2 each support three standard PCIe cards, while PCIe riser card assembly 3 is not utilized. The slots are labeled 1 to 6. Slots 1, 2, and 3 are located in PCIe riser card assembly 2. Slots 4, 5, and 6 are located in PCIe riser card assembly 1.

Figure 1-9 Appliance rear panel riser assembly locations



The following table describes the 3350 Appliance's standard PCIe-based I/O configuration.

Table 1-7 3350 Appliance standard PCIe-based I/O configuration

I/O configuration option	Slot 1 *	Slot 2	Slot 3	Slot 4 *	Slot 5	Slot 6
Standard	Intel RS3P4GF016J 12Gb SAS HBA [2]	Broadcom BCM957414A4142CC Dual 10/25 Gbe NIC adapter[3]	Broadcom BCM957414A4142CC 10/25 GbE NIC	RS3P4GF016J 12Gb SAS HBA [2]	Empty	Empty

* The 12Gb SAS HBA ports in slots 1 and 4 are used to connect the 3350 Appliance compute node to the Veritas 5U84 Primary Storage Shelf.

PCIe card cable connection types:

[1] Direct-Attach copper cable (also called a Twinaxial cable or Twinax)

[2] Standard copper

See "Total 3350 Appliance on-board and PCIe-based I/O ports" on page 24.

Total 3350 Appliance on-board and PCIe-based I/O ports

The following table shows the total number of I/O ports that are available with the 3350 Appliance.

Table 1-8 Total number of available 3350 Appliance on-board and PCIe-based I/O ports

I/O Configuration option	12Gb SAS HBA PCIe ports (copper)	10/25Gb Ethernet PCIe ports (optical)	1Gb Ethernet NIC on-board ports (copper)
Standard	4 per SAS HBA card, of which two are not usable See "SAS3 host bus adapter connector locations and labels" on page 27.	2	4

Intel RS3P4GF016J SAS3 RAID PCIe host bus adapter

Two Intel RS3P4GF016J SAS3 12Gb RAID PCIe host bus adapters provide a data path from the 3350 Appliance compute nodes to the 5U84 Primary Storage Shelf. SAS3 cables connect the SAS3 RAID PCIe host bus adapters to the 5U84 Primary Storage Shelf RAID controllers.

Table 1-9 Intel RS3P4GF016J SAS3 RAID PCIe HBA specifications

Item	Specification	
Bracket height	Full height	
System interface type	PCIe x8 Gen4	
Speed and slot width	8.0GT/s, 8-lane	
I/O processor module	SAS3816	
Output type	16x SAS 12Gbps	
Air flow (minimum)	0 LFM	
Operating temperature	10 to 55 C (50 to 131 F)	
Storage temperature	-40 to 70 C(-40 to 158 F)	
Storage humidity	Relative (non condensing): 20% - 80%; Storage: 5% - 95%	
Power consumption	State 1 (Watts) 8.74W	State 2 (Watts) 11.89W

Access 3350 12Gb SAS3 RAID host bus adapter	
SKU Number	**Description**
31968	HBA PCIE RS3P4GF016J CONTROLLER CARD FRU HARDWARE

3350 Appliance network interface card port assignments

The following section describes the on-board 1Gb network interface card (NIC) port assignments and the PCIe-based 10/25Gb NIC port assignments for the 3350 Appliance.

Figure 1-10 3350 Appliance compute node on-board NIC port assignments

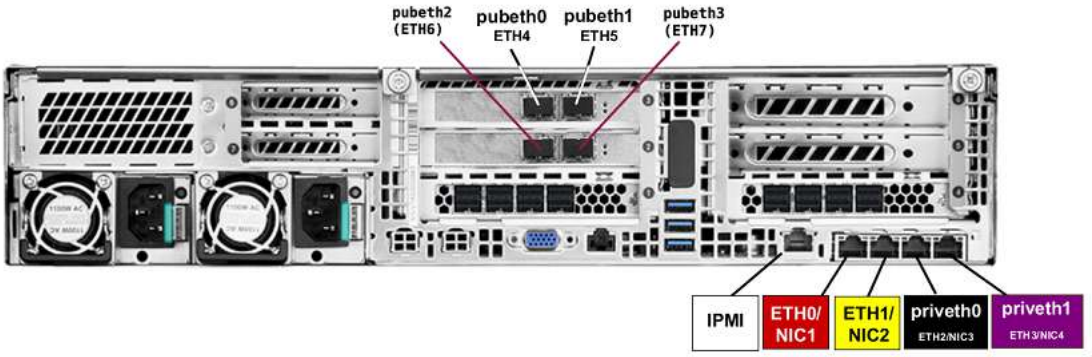


Table 1-10 Appliance compute node network interface port information

Port	Function
eth0/NIC1 (copper/RJ45 connector)	Used for management functions of the appliance. You can connect NIC1 (eth0) to an administrative network that does not provide any backup data transfer.
eth1/NIC2 (copper/RJ45 connector)	A 1-GbE port that can be configured as an administrative network port that does not provide any backup data transfer.
priveth0 (eth2/NIC3) (copper/RJ45 connector)	A 1-GbE private network port that is used for connections between the two appliance compute nodes
priveth1 (eth3//NIC4) (copper/RJ45 connector)	A 1-GbE private network port that is used for connections between the two appliance compute nodes.

Table 1-10 Appliance compute node network interface port information *(continued)*

Port	Function
IPMI port (copper/RJ45 connector)	A 1-GbE port that is used for appliance remote management purposes.
pubeth0 (eth4) *	A 10/25GbE port that is used for general network uses.
pubeth1 (eth5) *	A 10/25GbE port that is used for general network uses.
pubeth2 (eth6)*	A 10/25GbE port that is used for general network uses.
pubeth3 (eth7) *	A 10/25GbE port that is used for general network uses.

* Virtual IP addresses are assigned to the eth4 and eth6 ports of the appliance compute node during the initial configuration. IP addresses can be configured for ports eth5 and eth7 from the Access command-line interface after the initial configuration is complete. Ensure that eth4 and eth6 are plugged into the motherboard when you perform the initial configuration. eth5 and eth7 are optional and are not required to be plugged in.

SAS3 host bus adapter connector locations and labels

The 3350 Appliance uses two 12Gb SAS3 host bus adapters through which data is transferred from each of the 3350 Appliance compute nodes to the 5U84 Primary Storage Shelf. Each SAS3 host bus adapter connects to the 5U84 Primary Storage Shelf using mini-SAS cables. One of the SAS3 host bus adapters is installed in PCIe slot 1 of PCIe riser assembly 2. The other host bus adapter is installed in slot 4 of PCIe riser assembly 1.

The following picture and table provides more information about the SAS connectors.

Figure 1-11 SAS3 host bus adapter connector numbers and locations

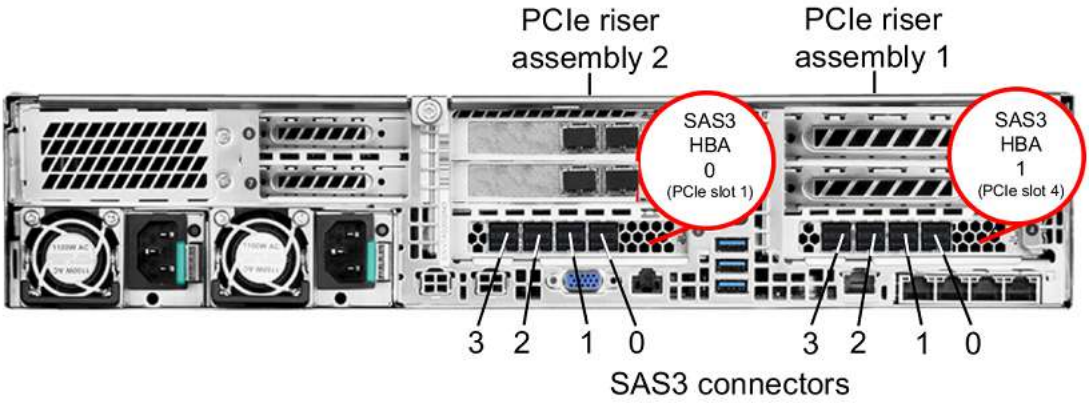


Table 1-11 SAS3 host bus adapter connector numbers and locations

Connector number	Connector location
Connector3 *(used for connections to the 5U84 Primary Storage Shelf)*	SAS3 host bus adapter 0 (PCIe slot 1)
Connector2 *(used for connections to the 5U84 Primary Storage Shelf)*	SAS3 host bus adapter 0 (PCIe slot 1)
Connector1 *(not used)*	SAS3 host bus adapter 0 (PCIe slot 1)
Connector0 *(not used)*	SAS3 host bus adapter 0 (PCIe slot 1)

Connector3 *(used for connections to the 5U84 Primary Storage Shelf)*	SAS3 host bus adapter 1 (PCIe slot 4)
Connector2 *(used for connections to the 5U84 Primary Storage Shelf)*	SAS3 host bus adapter 1 (PCIe slot 4)

Table 1-11 SAS3 host bus adapter connector numbers and locations *(continued)*

Connector number	Connector location
Connector1 *(not used)*	SAS3 host bus adapter 1 (PCIe slot 4)
Connector0 *(not used)*	SAS3 host bus adapter 1 (PCIe slot 4)

See “Intel RS3P4GF016J SAS3 RAID PCIe host bus adapter” on page 25.

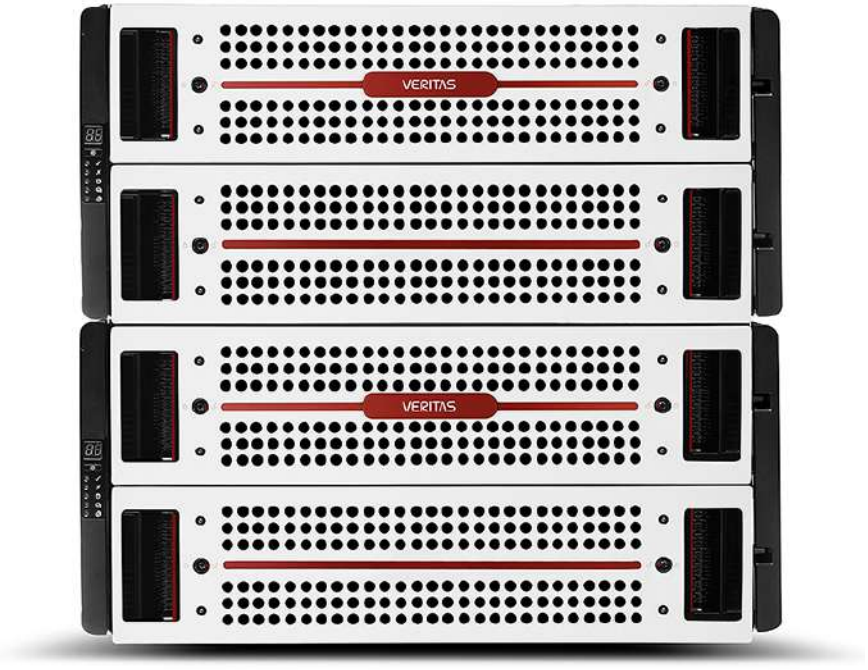
Chapter 2

About the Veritas 5U84 Storage Shelves

This chapter includes the following topics:

- About Veritas Access 3350 Appliance storage shelves
- About the 5U84 Primary Storage Shelf and 5U84 Expansion Storage Shelf rear components

About Veritas Access 3350 Appliance storage shelves



Veritas offers two external storage shelf models for the Veritas Access 3350 Appliance.

These include the:

- Veritas 5U84 Primary Storage Shelf (required)
- Veritas 5U84 Expansion Storage Shelf (optional)

Both of the 5U84 Storage Shelf chassis include a set of common internal core components, along with a set of plug-in modules.

The core components include:

- Two sliding disk drawers that contain Disk Drive In Carrier (DDIC) modules
- A front operations panel
- A front bezel

- Mid-plane printed circuit boards (PCB) that interface with controllers on the 5U84 Primary Storage Shelf and the 5U84 Expansion Storage Shelf.

In addition to the core components, the storage shelves also incorporate the following plug-in modules:

- Two 12Gb SAS-3 RAID controller modules (*5U84 Primary Storage Shelf only*)
- Two Storage Bay Bridge 2.1-compliant Expansion I/O controller modules (*5U84 Expansion Storage Shelf only*)
- Two power supply units (PSUs)
- Five fan modules
- 82 Disk Drive In Carrier (DDIC) modules with disk drives installed
- Two blank Disk Drive in Carrier (DDIC) modules
- A rail kit for rack mounting

The 5U84 Primary Storage Shelf and the 5U84 Expansion Storage Shelf each use a 5U chassis. Each chassis contains two sliding disk drive drawers that are located in the front of the storage shelf. Each drawer holds 41 Disk Drive In Carrier (DDIC) modules. The DDIC modules are installed in the drive drawer slots, which hold a total of 82 disk drives. Each DDIC module holds a 7200 rpm SAS-3-based disk drive with a capacity to hold either 4 TB or 10 TB of data. The disk drives and the DDIC modules are hot-swappable and can be replaced on-site while the storage shelf is operational.

Note: Each storage shelf drawer must be populated with disk drives of the same capacities. A mix of storage shelves, with different capacities in separate storage shelves is not supported.

In each storage shelf, two of the disk drives are used as global hot spares. Using 10-TB disk drives, a storage shelf provides 636.3TiB (700 TB) of usable data storage capacity. Using 4-TB disk drives, a storage shelf provides 254.4TiB (280 TB) of usable data storage capacity. The storage shelf disk drives are arranged in five RAID 6 sets, each comprised of 16 disk drives. These disks are used for AdvancedDisk data storage purposes. Depending on the storage configuration you purchase, the Access 3350 Appliance storage system supports up to 2.8PB of usable data storage space.

See “Available appliance storage options” on page 33.

Available appliance storage options

The Veritas Access 3350 Appliance compute nodes do not contain internal disk space on which to store data. Instead, the 3350 Appliance system uses one required Veritas 5U84 Primary Storage Shelf and up to three optional 5U84 Expansion Storage Shelves as the main data storage devices. The 5U84 Primary Storage Shelves connect to 3350 Appliance compute nodes and use RAID 6 drive sets to protect the stored data.

Note: RAID 6 is also known as double-parity RAID. It uses two parity stripes on each disk to protect data. RAID 6 allows for two hard disk failures within the RAID disk array before any data is lost.

Refer to the following table for available storage capacity for the 3350 Appliance using 4-TB and 10-TB disk capacities.

Note: Each storage shelf must contain disk drives of the same capacity. Veritas does not support mixing 4-TB and 10-TB disk drives within a storage shelf.

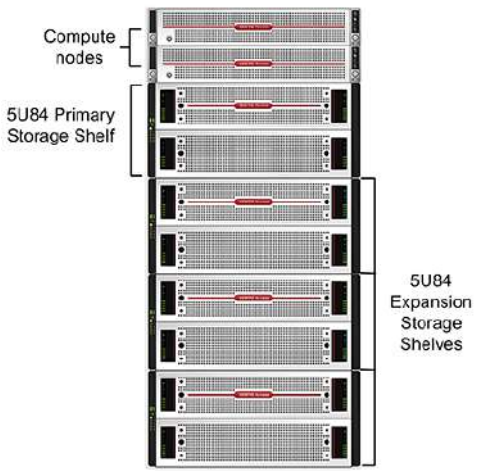
Table 2-1 Available usable storage capacities for a 3350 Appliance system using 4-TB and 10-TB disk drives

Drive size	Storage Shelf usable storage capacity	One storage shelf (one Primary Shelf)	Two storage shelves (one Primary shelf; one Expansion shelf)	Three storage shelves (one Primary shelf; two Expansion shelves)	Four storage shelves (one Primary shelf; three Expansion shelves)
4 TB	254.4 TiB (280 TB)	254.4 TiB (280 TB)	4-TB drive expansion: 510 TiB (560 TB) 10-TB drive expansion: 891 TiB (980 TB)	4-TB drive expansion: 764 TiB (840 TB) 10-TB drive expansion: 1528 TiB (1680 TB)	4-TB drive expansion: 1018.6 TiB (1120 TB) 10-TB drive expansion: 2165 TiB (2380 TB)

Table 2-1 Available usable storage capacities for a 3350 Appliance system using 4-TB and 10-TB disk drives *(continued)*

Drive size	Storage Shelf usable storage capacity	One storage shelf (one Primary Shelf)	Two storage shelves (one Primary shelf; one Expansion shelf)	Three storage shelves (one Primary shelf; two Expansion shelves)	Four storage shelves (one Primary shelf; three Expansion shelves)
10 TB	636 TiB (700 TB)	636 TiB (700 TB)	4-TB drive expansion: 891 TiB (980 TB) 10-TB drive expansion: 1272 TiB (1400 TB)	4-TB drive expansion: 1146 TiB (1260 TB) 10-TB drive expansion: 1908 TiB (2100 TB)	4-TB drive expansion: 1401 TiB (1540 TB) 10-TB drive expansion: 2544 TiB (2800 TB)

Note: 3350 Appliance systems that use up to four storage shelves for increased storage capacity can be installed in a single hardware rack.



See the *Veritas Access 3350 Appliance Hardware Installation Guide* for more information.

To determine the hardware configuration for the storage capacities that your environment requires, contact your Veritas sales representative, or your Veritas Partner representative.

About the Veritas 5U84 Storage Shelf disk drive drawers

This section discusses the 5U84 Primary Storage Shelf and 5U84 Expansion Storage Shelf disk drive drawers and the components that comprise the drawers.

Disk drive drawers

Figure 2-1 5U84 Primary Storage Shelf/5U84 Expansion Storage Shelf disk drive drawer

The 5U84 Primary Storage Shelf and the 5U84 Expansion Storage Shelf each use a 5U chassis. Each chassis contains two sliding drawers that are accessible from the front of the storage shelves. Each drawer can hold 42 Disk Drive In Carrier (DDIC) modules. The DDIC modules are installed in each of the drive drawer slots, which can hold a total of 84 disk drives. Each DDIC module holds one 3.5" SAS-3, 7200 rpm hard disk drive, in either 4-TB or 10-TB capacities. The disk drives and the DDIC modules are hot-swappable and can be replaced on-site while the storage shelf is operational.

Disk drive slot numbering

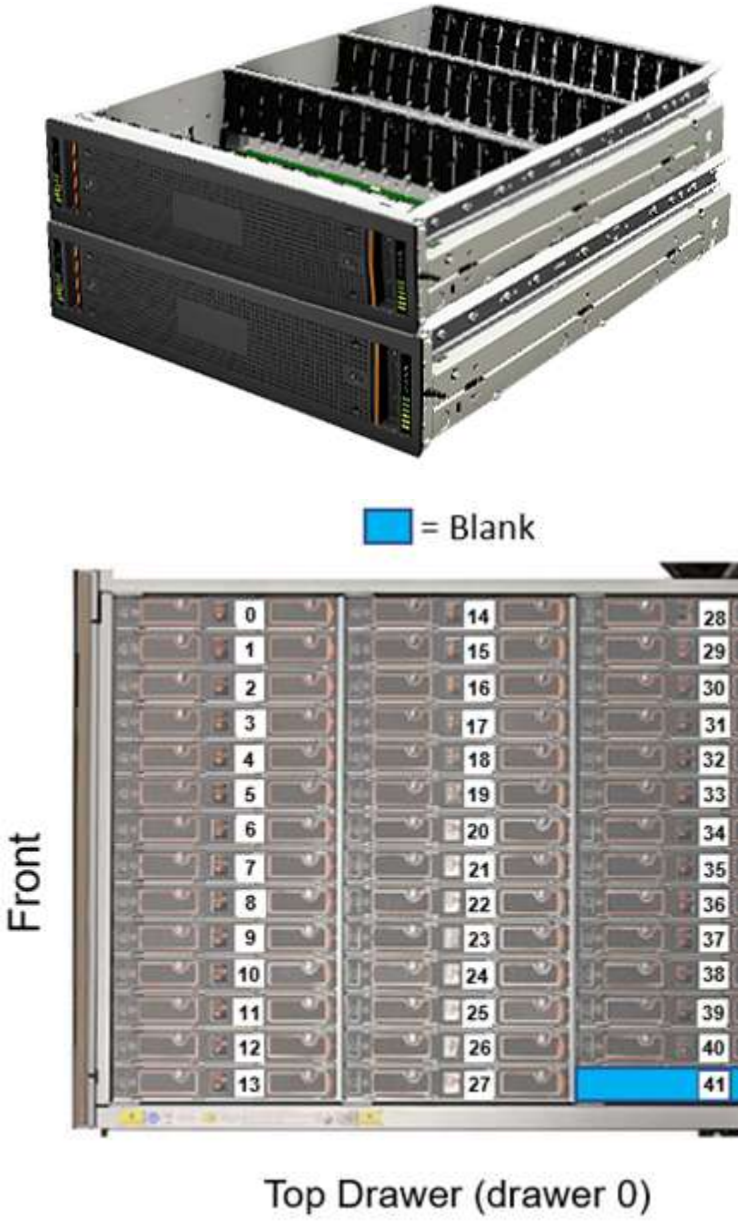
Each disk drive drawer in a 5U84 storage shelf is divided into three compartments. The compartments contain the individual drive slots that hold the DDIC modules and the disk drives.

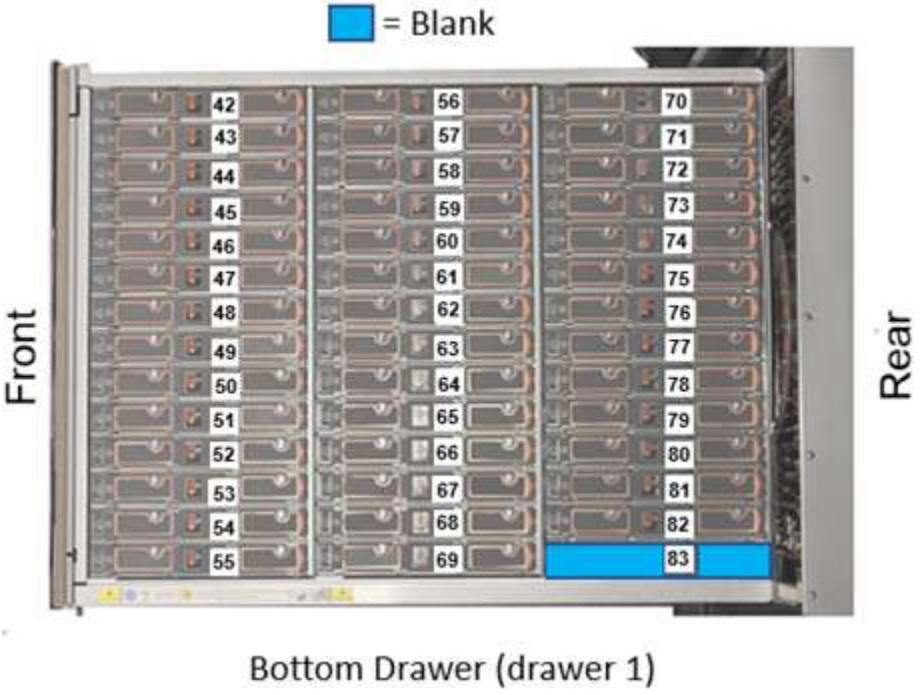
In the top drive drawer, the drive slots are numbered from left to right, beginning with the first compartment that is closest to the front panel. The drive slots in this compartment are numbered 0 to 13. The drive slots in the second compartment are in the middle of the drive drawer. These slots are numbered 14 to 27. The drive slots in third compartment are closest to the rear of the shelf. These slots are numbered 28 to 41.

In the bottom drive drawer, the drive slots are numbered from left to right, beginning with the first compartment that is closest to the front panel. The drive slots in this compartment are numbered 42 to 55. The drive slots in the second compartment are in the middle of the drive drawer. These slots are numbered 56 to 69. The drive slots in third compartment are closest to the rear of the shelf. These slots are numbered 70 to 83.

See Figure 2-2 on page 37.

Figure 2-2 Disk drive slot numbering





Disk Drive In Carrier (DDIC) modules

All storage shelf hard disk drives are housed in DDIC modules. Each disk drive drawer accepts a Disk Drive In Carrier (DDIC) module for each disk drive slot in the drawer. DDIC modules enable disk drives to be quickly inserted and removed without turning off the 5U84 storage shelves. In addition, each DDIC prevents mis-alignment and damage to the disk drive connectors during the disk drive insertion and removal process.

For troubleshooting purposes, DDIC modules provide one amber drive fault LED indicator per disk drive. The fault indicator enables you to easily identify a failed drive carrier in the drive drawer. You can see drive fault LED indicator when the disk drive drawer is open.

Figure 2-3 Disk Drive In Carrier (DDIC) module

Figure 2-4 Disk Drive In Carrier (DDIC) module components and locations

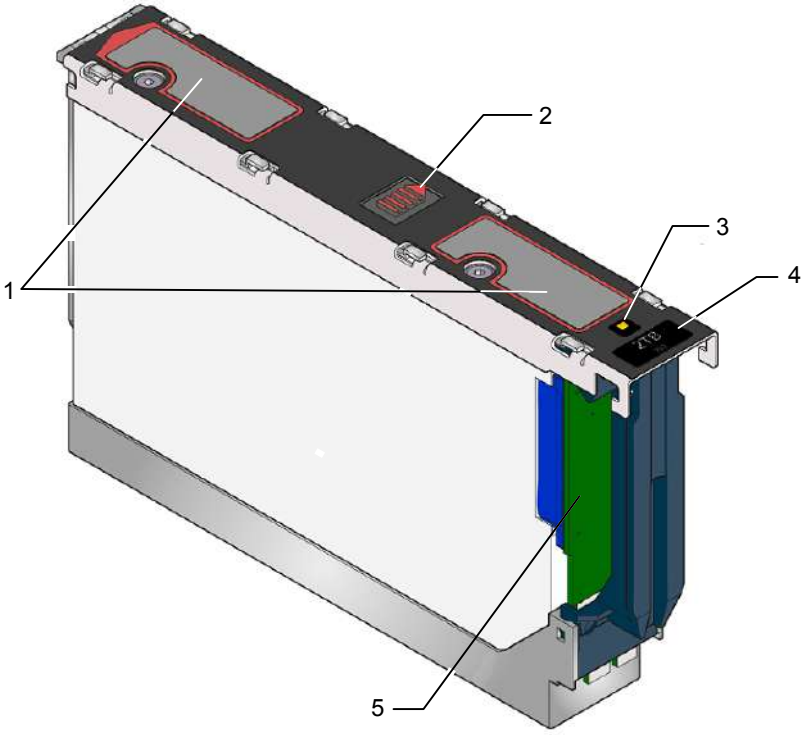


Table 2-2 5U84 Storage Shelf DDIC component locations

Number	Component
1	Touch points **Note:** Touch points are used to facilitate the removal of the DDIC module from the storage shelf drawer.
2	Latch button
3	Drive Fault LED
4	Disk drive capacity label
5	Dongle

Disk Drive Drawer printed circuit board (PCB) assemblies

Each disk drive drawer in a 5U84 storage shelf uses a printed circuit board (PCB) assembly to provide the electrical connectivity to the drawer's disk drives.

Along with providing the electrical connectivity to the disk drives, PCB assemblies also provide:

- Mounting platforms for the drawer cabling system
- Redundant power paths to each disk drive
- Redundant 12Gb/s SAS signal paths to each disk drive
- Provide technical feedback to the system when a drawer is opened or closed.

PCB assemblies include the following components:

- Three drawer Baseplane cards
- One right side Drawer Sideplane card
- One left side Drawer Sideplane card

Figure 2-5 Disk Drive Drawer PCB assembly

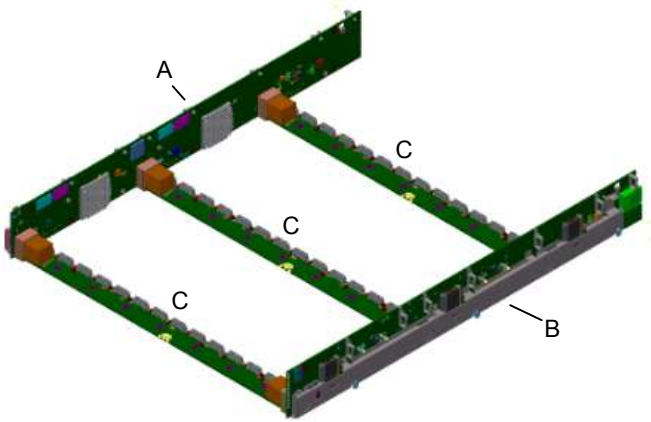


Table 2-3 Disk drive drawer PCB assembly components

Label	Item
A	Drawer Sideplane card (left)
B	Drawer Sideplane card (right)
C	Baseplane card

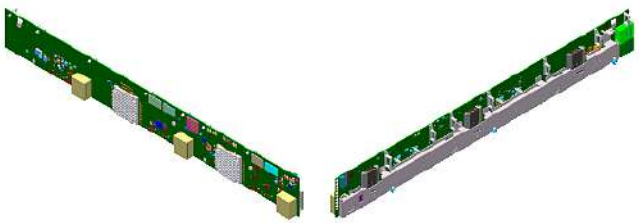
Each PCB assembly contains two Drawer Sideplane cards. One Sideplane card mounts on the right side of the disk drawer, while the other card mounts on the left side of the drawer.

Drawer Sideplane cards provide power paths to the drawer Baseplanes and the DDICs and their installed disk drives. Sideplane cards also provide 12Gb/s SAS connections.

Sideplane cards are hot swappable and replaceable by service personnel while the storage shelf is running in a rack.

Note: Removing the Sideplane upper metal cover removes power to the Sideplane, which enables the faulty Sideplane to be hot-swapped.

Figure 2-6 Inside and outside views of a right side Sideplane card



Three Drawer Baseplanes comprise each PCB assembly. Drawer Baseplanes provide a dual path for 12Gb/s SAS connectivity between the Drawer Sideplane cards and the DDICs. They also provide power to the DDICs from either the right or the left Drawer Sideplane cards.

The Drawer Baseplanes also provide four remote temperature sensing diodes that monitor disk drive temperatures within the disk drive drawers.

Figure 2-7 Drawer Baseplane example

Drawer Sideplane Status panels

Drawer Sideplane Status panels are located on the front of the 5U84 storage shelves. These panels provide status and the activity information about the Sideplane card.

Figure 2-8 Drawer Sideplane Status panel locations

Figure 2-9 5U84 Primary Storage Shelf / 5U84 Expansion Storage Shelf Drawer Sideplane Status panel

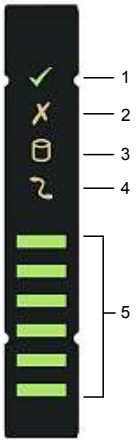


Table 2-4 Drawer Sideplane Status panel descriptions

Number	Item
1	Sideplane card OK / Power good
2	Sideplane card Fault
3	Logical Fault
4	Cable Fault
5	Activity Bar Graph

The following table describes the Drawer Sideplane LED statuses.

Table 2-5 Drawer Sideplane LED statuses

Status	Power (Green)	Drawer Fault (Amber)	Cable Fault (Amber)	Logical Fault (Amber)	Activity Bar Graph (Green)
Drawer Sideplane card OK / Power Good	On	Off	Off	Off	X
Drawer Sideplane card Fault	Off	On	X	X	Off

Table 2-5 Drawer Sideplane LED statuses *(continued)*

Status	Power (Green)	Drawer Fault (Amber)	Cable Fault (Amber)	Logical Fault (Amber)	Activity Bar Graph (Green)
Drive failure has occurred causing loss of availability or redundancy	On	On	X	X	X
Array in impacted state (SES) Indicated	On	X	X	Flashing	X
Cable Fault	Off	X	On	X	Off
Drive Activity	On	Off	Off	Off	On *

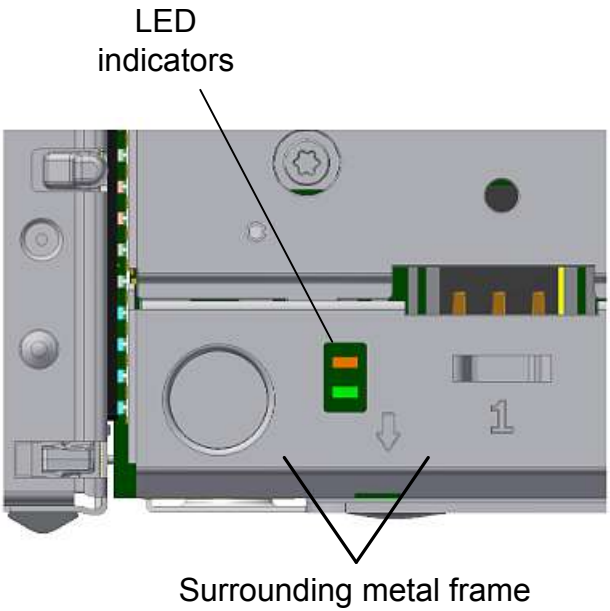
X = Disregard

* The Activity Bar Graph is a six-segment indicator that shows activity of the SAS disk drive interface to the Sideplane. If none of the segments are lit, then there is no SAS disk drive activity occurring. Increasing disk drive activity is measured upward, starting with the bottom segment. When full disk drive activity occurs, all six segments are lit.

Drawer Sideplane hot swap LED indicators

Drawer Sideplane hot-swap LED indicator lights are mounted on each drawer's Sideplane printed circuit board assembly. They are visible through each Sideplane's metal frame when the drawer is open.

Figure 2-10 Drawer Sideplane hot-swap LED location



The following table describes the Drawer hot-swap Sideplane LED indicator statuses.

Table 2-6 Drawer Sideplane Hot-swap LED indicator statuses

Status	12V Power LED (Green)	Power disabled LED (Amber)
Sideplane 12V power present (DO NOT hot-swap the sideplane)	On	X
Sideplane 12V is disabled (OK to hot-swap the Sideplane)	Off	On
X = Disregard		

5U84 Primary Storage Shelf and the 5U84 Expansion Storage Shelf control panel

The control panel is installed on the left side of both the 5U84 Primary Storage Shelf and the 5U84 Expansion Storage Shelf. It is functionally the same for both systems.

Figure 2-11 Control panel location

Figure 2-12 Control panel

The following table describes the control panel functions.

Table 2-7 Control panel functions and descriptions

Number	Function	Description
1	Unit Identification Display	The Unit Identification Display is a dual digit display that provides information about the storage shelf. Its primary function is to assist in the configuration of multiple storage shelves that are connected to the appliance.
2	Input button	The Input button enables you to set the Unit Identification display number.
3	Power On / Standby LED (Green or Amber)	The Power On/Standby LED shows Amber when only standby power is available. Otherwise, the LED shows Green when system power is available.
4	Module Fault LED (Power Cooling Module, I/O module status) (Amber)	The Module Fault LED illuminates when there is a system hardware fault. The system hardware fault may be associated with a fault LED on a Power Cooling Module (PCM) or on an I/O module.
5	Logical Fault LED (Amber)	The Logical Status LED shows a change of status or a fault. Typically these changes of status or faults are associated with the shelf's disk drives. However, the Logical Status LED can also indicate an issue with an internal RAID controller or external RAID controller, or with a host bus adapter.
6	Top Drawer Fault (Amber)	The Top Drawer Fault LED (drawer 1) shows a change of status or a fault with the top disk drive drawer in the storage shelf.
7	Bottom Drawer Fault (Amber)	The Bottom Drawer Fault LED (drawer 2) shows a change of status or a fault with the bottom disk drive drawer in the storage shelf.

About the 5U84 Primary Storage Shelf and 5U84 Expansion Storage Shelf rear components

This section describes the rear components of the 5U84 Primary Storage Shelf and 5U84 Expansion Storage Shelf.

The 5U84 Primary Storage Shelf and the 5U84 Expansion Storage Shelf contain the following removable rear components:

- SAS-3 RAID Controllers *(5U84 Primary Storage Shelf only)*
- Expansion I/O modules *(5U84 Expansion Storage Shelf only)*

- Fan modules
- Power Supply Units (PSUs)

Figure 2-13 5U84 Primary Storage Shelf rear components

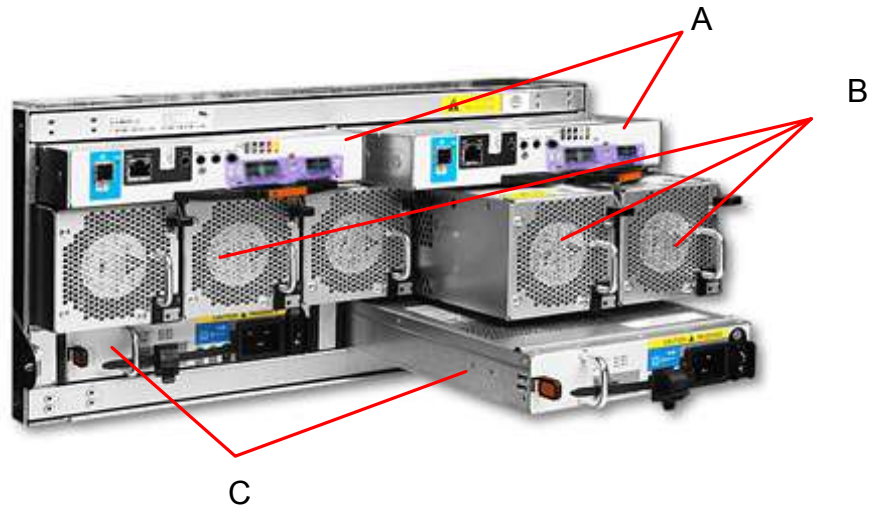


Table 2-8 5U84 Primary Storage Shelf rear component locations

Letter	Item
A	RAID Controllers (from left to right) RAID Controller A, RAID Controller B
B	Fan modules (from left to right) Fan Module 0, Fan Module 1, Fan Module 2, Fan Module 3, and Fan Module 4
C	Power Supply Units (from left to right) PSU 0, PSU 1

Figure 2-14 5U84 Expansion Storage Shelf rear components

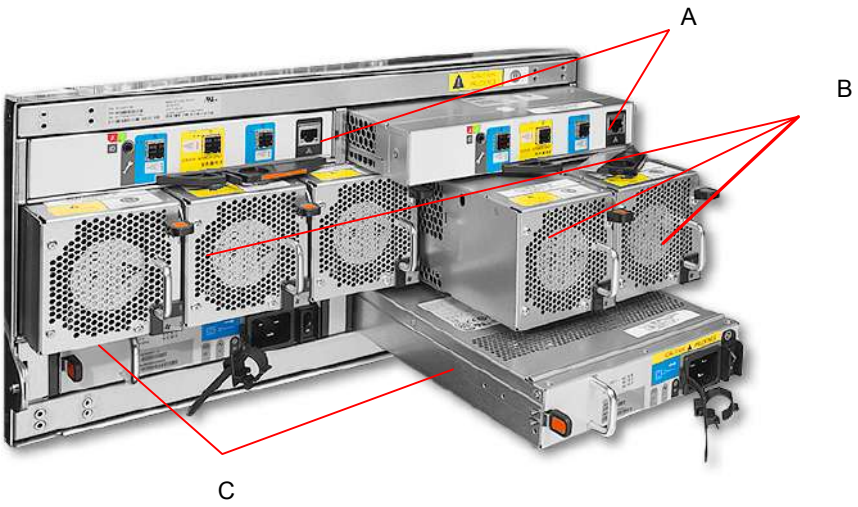


Table 2-9 5U84 Expansion Storage Shelf rear component locations

Letter	Item
A	Expansion I/O modules (from left to right) Expansion I/O Module A, Expansion I/O Module B
B	Fan modules (from left to right) Fan Module 0, Fan Module 1, Fan Module 2, Fan Module 3, and Fan Module 4
C	Power Supply Units (from left to right) PSU 0, PSU 1

5U84 Primary Storage Shelf

The 5U84 Primary Storage Shelf uses two SAS-3 RAID controllers, which are located in the top two slots of the back panel. The RAID controllers provide RAID data protection technology for the data that is stored on the 5U84 Primary Storage Shelf disk drives. The RAID controllers also provide RAID data protection technology for the optional 5U84 Expansion Storage Shelves that you connect to the 5U84 Primary Storage Shelf.

SAS-3 copper cables connect the 3350 Appliance compute nodes to the 5U84 Primary Storage Shelf through the storage shelf's RAID controllers.

Five high performance fan modules connect to the storage shelf's midplane connector through the middle slots. Each fan module contains two contra-rotating high performance fans, along with separate power and control circuits for each internal fan.

Two redundant Power Supply Units (PSUs) are located in slots beneath the fan modules.

To operate, the 5U84 Primary Storage Shelf must have at least one functioning RAID controller, one functioning power supply unit, and four functioning fan modules.

5U84 Expansion Storage Shelf

The 5U84 Expansion Storage Shelf uses two Expansion I/O modules, which are located in the top two slots of the back panel. The Expansion I/O modules provide SAS-3 I/O data transfers between the 5U84 Primary Storage Shelf and the 5U84 Expansion Storage Shelf. The Expansion I/O modules also provide I/O data transfers between the first 5U84 Expansion Storage Shelf and up to two additional 5U84 Expansion Storage Shelves.

SAS-3 cables connect the 5U84 Expansion Storage Shelf to the 5U84 Primary Storage Shelf through the 5U84 Expansion Storage Shelf's Expansion I/O modules. SAS-3 cables are also used to daisy chain up to two additional 5U84 Expansion Storage Shelves to the first 5U84 Expansion Storage Shelf.

Five high performance fan modules connect to the storage shelf's midplane connector through the middle slots. Each fan module contains two contra-rotating, high performance fans, along with separate power and control circuits for each internal fan. The device must have at least one functioning RAID controller, one functioning power supply module, and one functioning fan module.

Two redundant Power Supply Units (PSUs) are located in slots beneath the fan modules.

To operate, the 5U84 Expansion Storage Shelf must have at least one functioning Expansion I/O module, one functioning PSU, and four functioning fan modules.

See “Veritas 5U84 Expansion Storage Shelf Expansion I/O modules” on page 55.

Veritas 5U84 Primary Storage Shelf RAID controllers

The Veritas 5U84 Primary Storage Shelf uses dual, hot swappable SAS-3 RAID controllers. These controllers create and manage the 5U84 Primary Storage Shelf disk drive RAID sets that contain backed up data. They also create and manage the RAID sets on 5U84 Expansion Storage Shelves when those are attached to the 5U84 Primary Storage Shelf.

The SAS-3 RAID controllers run RAID level 6 on the storage shelf. RAID 6 offers the highest level of data protection. It allows simultaneous write operations, while

also allocating two sets of parity data across the drives that comprise the RAID 6 array.

The SAS-3 RAID controllers also provides an additional SAS-3 port. The SAS-3 port enables data to flow at SAS-3 data transfer rates between the 5U84 Primary Storage Shelf and the first optional 5U84 Expansion Storage Shelf.

Figure 2-15 Veritas 5U84 Primary Storage Shelf SAS-3 RAID controllers

The following figure and table provides component details for the Veritas 5U84 Primary Storage Shelf SAS-3 RAID controller modules.

Figure 2-16 Veritas 5U84 Primary Storage Shelf SAS-3 RAID Controller components and locations

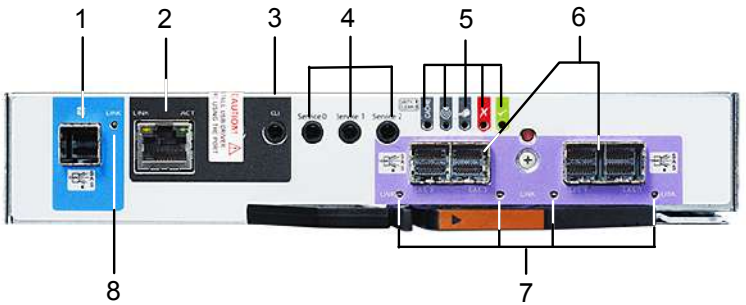


Table 2-10 Veritas 5U84 Primary Storage Shelf SAS-3 RAID Controller components

Number	Component
1	Expansion SAS port
2	Ethernet port **Note:** Veritas does not use or support the Ethernet port.
3	USB port
4	Serial ports (Service only)
5	Indicator LEDs
6	SAS-3 RAID ports - connects to the 3350 Appliance compute nodes
7	Activity LEDs
8	Expansion SAS port Status

Figure 2-17 Veritas 5U84 Primary Storage Shelf SAS-3 RAID Controller indicator LED details

Table 2-11 Veritas 5U84 Primary Storage Shelf SAS-3 RAID Controller indicator LED details

LED	Description	Definition
1	Host 12Gb SAS-3 Link Status/Link Activity	Off - No link detected. Green- The port is connected and the link is up. Amber - Partial link exists (one or more lanes are down) Blinking green or amber- The link has I/O activity.

Table 2-11 Veritas 5U84 Primary Storage Shelf SAS-3 RAID Controller indicator LED details *(continued)*

LED	Description	Definition
2	OK	Off - A controller issue has been detected, or the controller is turned off. Blinking green - The system is starting. Green - The controller is operating normally.
3	Fault	Off - The controller is operating normally. Amber - A controller fault has been detected or a service action is required. Blinking amber - Hardware-controller power on error, or a cache flush or restore error.
4	OK to Remove	Off - The controller is not prepared for removal. Blue - The controller is prepared for removal.
5	Identify	White - The controller is being identified.
6	Cache Status	Off - In a working controller, the cache is clean (contains no unwritten data). This is an occasional condition that occurs while the system is booting. Green - The cache is dirty (contains unwritten data) and the operation is normal. The unwritten information can be the log data or the debug data that remains in the cache. By itself, a Green cache status LED does not indicate that any user data is at risk or that any action is necessary. Blinking Green - A Compact Flash flush or a cache self-refresh is in progress, indicating cache activity.
7	Network Port Link Activity Status *	Off - The Ethernet link is not established, or the link is down. Green - The Ethernet link is up (applies to all negotiated link speeds).
8	Network Port Link Speed *	Off - The link is up at 10/100base-T negotiated speeds. Amber - The link is up and negotiated at 1000base-T speed.
9	SAS-3 Expansion Port Status	Off - The port is empty or the link is down. Green - The port is connected and the link is up.

Table 2-11 Veritas 5U84 Primary Storage Shelf SAS-3 RAID Controller indicator LED details *(continued)*

LED	Description	Definition
* When port is down, both LEDs are off		

Veritas 5U84 Expansion Storage Shelf Expansion I/O modules

Veritas 5U84 Expansion Storage Shelf Expansion I/O modules provide SAS-3 data throughput and communications between one or more 5U84 Expansion Storage Shelves.

Figure 2-18 Veritas 5U84 Expansion Storage Shelf Expansion I/O module

Figure 2-19 Veritas 5U84 Expansion Storage Shelf Expansion I/O module

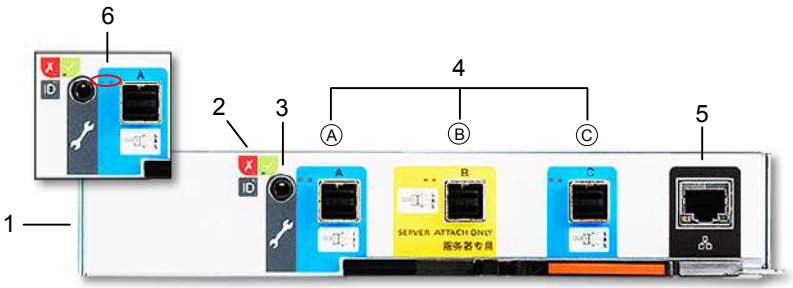


Table 2-12 Expansion I/O module components and locations

Number	Component
1	Expansion I/O module
2	Expansion I/O module Status LEDs
3	RS232 jack (debugging purposes only)
4	SAS-3 ports - A, B, and C
5	Ethernet port **Note:** Veritas does not use or support the Ethernet port.
6	SAS Activity LEDs

Expansion I/O module Status LED location and conditions

This section discusses the location of the Status LEDs on the Expansion I/O modules and the Status LED conditions.

Figure 2-20 Expansion I/O module Status indicator LED location

Table 2-13 Expansion I/O module icon and Status LED conditions

Condition	Activety LED (green)	Fault LED (amber)
Module Fault (amber)	On Off	The Expansion I/O module has encountered a fault condition. The Expansion I/O module is operating normally.

Table 2-13 Expansion I/O module icon and Status LED conditions *(continued)*

Condition	Activety LED (green)	Fault LED (amber)
Power (green)	On Off	The Expansion I/O module is on. The Expansion I/O module is off.
ID (blue)	On	The Expansion I/O module is being identified.

Expansion I/O module SAS Activity LED location and conditions

This section discusses the location of the SAS Activity LEDs on the Expansion I/O modules and the SAS Activity LED conditions.

Figure 2-21 Expansion I/O module SAS Activity LED location

Table 2-14 Expansion I/O module SAS Activity LED conditions

Condition	Activity LED (green)	Fault LED (amber)
No Cable Present	Off	Off
Cable Present All links up, no activity.	On	Off
Cable Present All links up.	Flash with aggregate port activity	Off

Table 2-14 Expansion I/O module SAS Activity LED conditions *(continued)*

Condition	Activity LED (green)	Fault LED (amber)
Critical Fault ■ Any fault which causes operation of the cable to cease or fail to start For example, an OVERCURRENT trip. ■ No connection detected at the opposite end of the SAS cable	Off	On
Non-Critical Fault Any fault which does not cause the connection to cease operation. For example, not all links established; OVERTEMPERATURE condition detected.	Flash with aggregate port activity	Flashing - One second on; one second off

Veritas 5U84 Storage Shelf cooling modules

The Veritas 5U84 Storage Shelves include five cooling modules. The cooling modules provide cooling to the entire unit, which is suitable to maintain the internal component temperatures below each components maximum temperature limits.

Figure 2-22 Veritas 5U84 Storage Shelf cooling module components

Table 2-15 Veritas 5U84 Storage Shelf cooling module component locations

Number	Component
1	High performance, contra-rotating cooling fans
2	Release latch
3	Handle
4	Mid-plane connector

Cooling modules provide the following features:

- Fast removal and replacement times without the need to turn off the storage shelf.
- Electronic fan speed control to the fans.
- Redundant serial interface connections to the rest of the storage shelf system.
- Cooling module redundancy
- Redundancy includes:
  - Maintaining the cooling function of the cooling module in the event of a single fan rotor failure.
  - Maintaining the normal operation of the cooling module if one cooling control or fan controller module fails.
  - Automatically switching fan speeds to Full/High mode if the cooling module control unit fails.
  - Maintaining the normal operation of the storage shelf for two minutes when a cooling module is swapped out due to a failure.

5U84 Storage Shelf Power Supply Units

Veritas 5U84 Storage Shelves includes dual Power Supply Units (PSU) that provide redundant power to the storage shelves. If one PSU fails, the storage shelves continue to operate as the second PSU continues to supply the storage shelf with power.

PSUs are hot-swappable. You can replace a faulty PSU while the storage shelf is running. However, you must complete the PSU replacement procedure within **two minutes** after you remove the faulty PSU.

Veritas 5U84 Storage Shelf chassis are keyed to prevent PSUs from being inserted upside down.

Figure 2-23 5U84 Storage Shelf Power Supply Unit

The rear panel of the PSU includes a power switch, three status LEDs, and an AC socket for the power cord. The rear panel also includes a handle that you use during the PSU insertion and removal process.

Figure 2-24 5U84 Storage Shelf Power Supply Unit

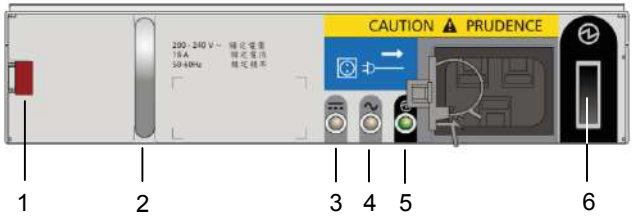


Table 2-16 5U84 Storage Shelf Power Supply Unit component locations

Number	Component
1	Release latch
2	Handle
3	PSU Fail LED
4	AC Fail LED
5	Power OK LED
6	Power switch

Chapter 3

Access 3350 Appliance and 5U84 Storage Shelf cables

This chapter includes the following topics:

- Power cables
- Network cable
- Multi-mode fiber optic cable
- SAS-3 cable
- Twinaxial copper cables

Power cables

Each of the AC power modules in both the Veritas Access 3350 Appliance and the required Veritas 5U84 Primary Storage Shelf accept one AC power cable. The optional 5U84 Expansion Storage Shelf also uses one AC power cord in each of its AC power modules. One end of the AC power cable connects to the power supply on the appliance or the storage device. The other end of the cable connects to an external Power Distribution Unit (PDU) on the rack.

Power cables include a live line, a neutral line, and a grounding line.

Veritas Access 3350 Appliance AC power cable

Figure 3-1 AC power cable - Veritas Access 3350 Appliance Appliance

A AC power connector (IEC-60320-C14) to an external power supply such as a Power Distribution Unit (PDU) on a rack.

B AC power connector (IEC-60320-C13) to an appliance.

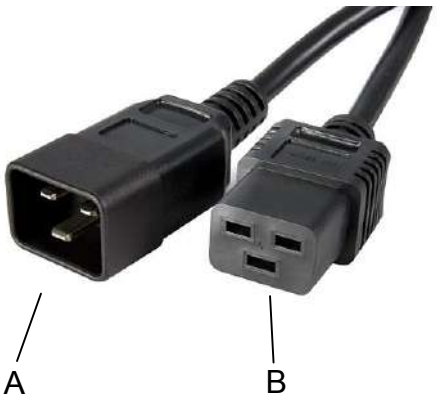
Cable rating: 15A 250V

Note: If your power distribution unit is not compatible with the IEC-60320-C14 plug, Veritas recommends that you purchase your power cable locally. Make sure that the power cable meets or exceeds the indicated power rating.

See " 3350 Appliance compute node technical specifications" on page 69.

Veritas 5U84 Primary Storage Shelf / Expansion Storage Shelf AC power cable

Figure 3-2 AC power cable - Veritas 5U84 Primary Storage Shelf / Expansion Storage Shelf



A AC power connector (IEC-60320-C20) to an external power supply such as a Power Distribution Unit (PDU) on a rack.

B AC power connector (IEC-60320-C19) to storage shelf.

Cable rating: 20A 250V

Note: If your power distribution unit is not compatible with the IEC-60320-C20 plug, Veritas recommends that you purchase your power cable locally. Make sure that the power cable meets or exceeds the indicated power rating.

See " Veritas 5U84 Storage Shelf technical specifications" on page 72.

See "Network cable" on page 64.

See "Multi-mode fiber optic cable" on page 64.

See "SAS-3 cable" on page 65.

See "Twinaxial copper cables" on page 67.

Network cable

The appliance communicates with the Ethernet networks through an Ethernet network cable. One end of the network cable connects to the management network port or service network port of the appliance. The other end of the cable connects to the network switch or an external gateway. Both ends of the cable are RJ45 connectors.

Figure 3-3 Network cable

See “Power cables” on page 61.

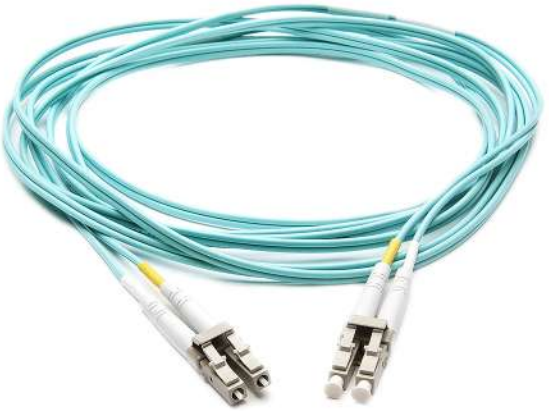
See “SAS-3 cable” on page 65.

See “Twinaxial copper cables” on page 67.

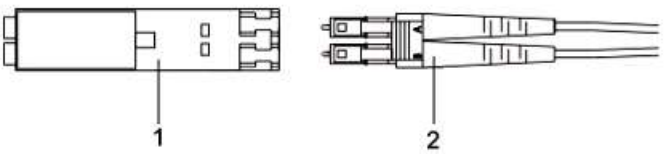
Multi-mode fiber optic cable

A Veritas &aModel; Appliance compute node communicates with the required 5U84 Primary Storage Shelf through multi-mode fiber optic cables. One end of each fiber optic cable connects to PCIe-based 16Gb Fibre Channel host bus adapters that are installed in the compute node. The other end of the fiber optic cable connects to the 5U84 Primary Storage Shelf's Fibre Channel RAID controller. Both ends of the fiber optic cable use LC connectors.

Figure 3-4 Multi-Mode fiber cable



Fiber optic cables require Small Form-factor Pluggable (SFP+) transceivers, which are provided with each device having Fibre Channel ports. The diagram shows the SFP, labeled 1, and the fiber optic cable which is attached to it, labeled 2.



Supported SFPs are listed:

- Finisar FTLX8574D3BCV
- Broadcom AFBR-710DMZ

See “Power cables” on page 61.

See “Network cable” on page 64.

See “SAS-3 cable” on page 65.

See “Twinaxial copper cables” on page 67.

SAS-3 cable

SAS-3 data cables are used to connect the Veritas 5U84 Primary Storage Shelf to the 3350 Appliance compute nodes. SAS-3 cables also connect multiple 5U84 Expansion Storage Shelves to each other. SAS-3 cables have SAS-3 connectors

on both ends. SAS-3 cables ship with each Veritas Appliance, and with each Veritas 5U84 Expansion Storage Shelf.

Figure 3-5 SAS-3 cable

See “Power cables” on page 61.

See “Network cable” on page 64.

See “Twinaxial copper cables” on page 67.

Twinaxial copper cables

See “Power cables” on page 61.

See “Network cable” on page 64.

See “Multi-mode fiber optic cable” on page 64.

See “SAS-3 cable” on page 65.

Appendix A

Technical specifications, Environmental/Protocol standards, and Compliance standards

This appendix includes the following topics:

- 3350 Appliance compute node technical specifications
- Veritas 5U84 Storage Shelf technical specifications
- Environmental specifications
- Protocol standards
- Regulatory, compliance, and certification information

3350 Appliance compute node technical specifications

Table A-1 3350 Appliance compute node technical specifications

Technical Specification	3350 Appliance compute node
Rack information	19" EIA standard The rack rails that are provided for the 3350 Appliance compute nodes are extensible to 32” (813 mm). This distance is the maximum depth that is allowed between rack posts. If the distance between rack posts is longer than 32” (813 mm) the rails and the appliance cannot be properly installed.
Processor	Two Xeon Silver 4210 CPUs
CPU speed	2.2 GHz (Turbo: 3.2 GHz)
Cores (each compute node)	20 (10 per processor)
Smart Cache	13.75MB Cache L3
System memory (per compute node)	Base memory capacity: 384GB Memory type: DDR4 LRDIMM Configuration: 6 x 64GB LRDIMM modules Operating voltage: 1.2V Configured clock speed: 2400MHz Maximum clock speed: up to 3200MHz
SAS RAID mezzanine card	Yes
SAS RAID PCIe card installed in a appliance compute node PCIe riser assembly	No
RAID levels	RAID1: 3350 Appliance compute node system disks **Note:** The RAID level is generated using an onboard Intel RMSHC080 RAID controller that is installed in each of the 3350 Appliance compute nodes.
Usable AdvancedDisk storage capacity (TB)	Usable AdvancedDisk storage capacity: up to 2544 TiB (2800 TB) See “Available appliance storage options” on page 33.

Table A-1 3350 Appliance compute node technical specifications *(continued)*

Technical Specification	3350 Appliance compute node	
Maximum number of storage shelves	4 One Veritas 5U84 Primary Storage Shelf; three Veritas 5U84 Expansion Storage Shelves	
I/O ports	12Gb SAS3 ports (PCIe-based)	8 total ports; four are used Used to connect the 3350 Appliance compute nodes to the 5U84 Primary Storage Shelf
	10/25Gb Ethernet PCIe card-based network interface cards	2 ports
	1Gb Ethernet ports	Four on-board ports
Dimensions (IEC rack compliant)	Appliance compute node: ■ Height: 8.89cm (3.5") (approximately 2U) ■ Width: 48.26cm (19") ■ Depth: 79.38cm (31.25") 5U84 Primary and 5U84 Expansion Storage Shelves: ■ Height: 21.97cm (8.65") (approximately 5U - shelf, overall) ■ Width: 48.26cm (19") (across the mounting flange) ■ Length/depth: 93.35cm (36.75") (from rear of the front flanges to the rear extremity of the chassis) **Note:** The Veritas 5U84 Primary Storage Shelf and the 5U84 Expansion Storage Shelf are longer than what a standard IEC-compliant rack normally supports. Due to the additional length, the rack-based PDU hardware may need to be installed on the outside of the rack to accommodate the storage shelves.	
Maximum weight	Appliance compute node: 23.26 kg (51.28 lbs)	
AC power requirements	Appliance compute node: 110 VAC - 220 VAC at 2.6 A	
Power factor	> 90%	

Table A-1 3350 Appliance compute node technical specifications *(continued)*

Technical Specification	3350 Appliance compute node
AC power cable	Specification: IEC-60320-C14 to IEC-60320-C13, 10A/250V, Black, 4 ft The IEC-60320-C14 plugs into a Power Distribution Unit. The IEC-60320-C13 plugs into an appliance or storage shelf power supply. The power supply unit is Lot 9 compliant. **Note:** If your power distribution unit is not compatible with the IEC-60320-C14 plug, then Veritas recommends that you purchase your power cable locally. Make sure the power cable meets or exceed the indicated power rating.
AC Frequency range	50/60Hz
Typical power consumption Maximum power consumption	260 watts 500 watts
Typical power consumption with a maximum of four external storage shelves	4,520 watts (two servers per cluster)
Maximum power consumption with a maximum of four external storage shelves	6,200 watts (two servers per cluster) (500 watts maximum per server)
System cooling requirement (heat dissipation) (Appliance with maximum storage shelves attached)	Typical: ■ 14,971 BTU/hour Maximum: ■ 20,291 BTU/hour
Operating voltage	100 VAC - 127 VAC 200 VAC - 240 VAC
Power conversion efficiency	90% +
Acoustic noise	70 dBA

See " Veritas 5U84 Storage Shelf technical specifications" on page 72.

See "Environmental specifications" on page 75.

See "Protocol standards" on page 75.

See "Regulatory, compliance, and certification information" on page 76.

Veritas 5U84 Storage Shelf technical specifications

The following table provides technical specifications for both the Veritas 5U84 Primary Storage Shelf and the Veritas 5U84 Expansion Storage Shelf.

Table A-2 Veritas 5U84 Primary Storage Shelf / 5U84 Expansion Storage Shelf technical specifications

Technical specification	Description
Rack information	The rack installation height is the space occupied by a storage shelf in a rack cabinet. The shelf fits into a 5U rack space. Install the storage shelf in a rack cabinet that is 19 inches (483mm) wide.
Dimensions (IEC rack compliant)	**5U84 Primary and 5U84 Expansion Storage Shelves** ■ Height: 21.97cm (8.65") (approximately 5U - shelf, overall) ■ Width: 48.26cm (19") (across the mounting flange) ■ Length/depth: 93.35cm (36.75") (from rear of the front flanges to the rear extremity of the chassis) **Note:** The Veritas 5U84 Primary Storage Shelf and the 5U84 Expansion Storage Shelf are longer than what a standard IEC-compliant rack normally supports. Due to the additional length, the rack-based PDU hardware may need to be installed on the outside of the rack to accommodate the storage shelves.
Hot swappable components	Disk drives, power supply units (PSUs), cooling modules, SAS Controllers, Expansion I/O modules
Usable storage capacity	Up to 2,544TiB (2,800TB), depending on the hardware configuration you purchase See "Available appliance storage options" on page 33.
Maximum weight	5U84 Primary Storage Shelf: 135 kg (298 lbs) with drives; no rail kit 5U84 Expansion Storage Shelf: 135 kg (298 lbs) with drives; no rail kit
Device types supported	Dual ported 12Gb/s SAS
Maximum drives per storage shelf	82

Table A-2 Veritas 5U84 Primary Storage Shelf / 5U84 Expansion Storage Shelf technical specifications *(continued)*

Technical specification	Description
Typical power consumption	1000 watts per storage shelf **Note:** You can connect a maximum of four storage shelves to the 3350 Appliance compute nodes.
Maximum power consumption	1300 watts per storage shelf
Supported RAID level	RAID6: 5U84 Primary Storage Shelf and 5U84 Expansion Storage Shelf data storage disks
Controllers	5U84 Primary Storage Shelf: Dual RealStor 5005 12Gb SAS RAID controllers per storage shelf 5U84 Expansion Storage Shelf: Dual Storage Bridge Bay (SBB) 2.1 compatible Expansion I/O modules per storage shelf
Host/Expansion Interface	Three universal x4 12Gb mini-SAS connectors (SFF-8644) per Expansion I/O module
Maximum output power	1300 watts maximum continuous output power at high line voltage You can connect up to four storage shelves to the 3350 Appliance compute nodes.
AC power requirements	200 - 240 VAC @ 6.67 A
Operating voltage	200V - 240 VAC
AC power cable	Specification: IEC-60320-C20 to IEC-60320-C19, 20A/250V, Black, 4ft The IEC-60320-C20 plugs into a Power Distribution Unit (PDU) on a rack. The IEC-60320-C19 plugs into an appliance or a storage shelf power supply. **Note:** If your power distribution unit is not compatible with the IEC-60320-C20 plug, Veritas recommends that you purchase your power cable locally. Make sure the power cable meets or exceed the indicated power rating.
AC Frequency range	50/60Hz

Table A-2 Veritas 5U84 Primary Storage Shelf / 5U84 Expansion Storage Shelf technical specifications *(continued)*

Technical specification	Description
Power conversion efficiency	81% @ 10% load 89% @ 20% load 93% @ 50% load 90% @ 100% load
Temperature range	Operating: 5º to 35ºC (de-rate 5ºC above 2,133m (7,000')) (41°F TO 95°F) Non-operating: -40°C to 70°C (-40°F TO 158°f)
Relative humidity	Operating: 20%rh to 80%rh non-condensing Non-operating: 5%rh to 100%rh non-condensing
Acoustic noise	82 dBA Sound Power Operating ≤ 8.0 Bels LWAd @ 23°
Operating altitude	-30 to 3048m (-100 to 10000ft) De-rate 5°C above 2134m (7000ft)
Non-operating altitude	-305 to 12192m (-1000 to 40000ft)
Operational vibration	0.21gRMS 5-500Hz Random
Operational shock	5g10ms ½ Sine
Relocation vibration (Non-operational)	0.3g2-200-2Hz Swept Sine.
Non-operational vibration	1.04 gRMS 2-200Hz Random.
Non-operational shock	30g10ms ½ Sine (Z-axis) 20g10ms ½ Sine(X-and Y-axes)

See " 3350 Appliance compute node technical specifications" on page 69.

See "Environmental specifications" on page 75.

See "Protocol standards" on page 75.

See "Regulatory, compliance, and certification information" on page 76.

Environmental specifications

Veritas Appliance compute node environmental specifications

Table A-3 Veritas Appliance compute node environmental specifications

Specification	
Operating temperature	ASHRAE A2 (10°C to 35°C) (50°F to 95°F)
Non-operating temperature	-25°C to 70°C (-14°F to 158°F) The non-operating temperature is defined as the temperature of the system when the system is turned off. It is also referred to as the storage temperature. Veritas recommends that you do not store the system in an environment where the temperatures fall outside of the listed temperature range.
Operating humidity (RH)	20% RH to 80% RH
Non-operating humidity	8% RH to 90% RH
Operating altitude (feet)	-30 to 3000 m with ASHRAE A2 class derating (0 to 10,000 ft)
Temperature gradient (per hour)	10°C/h (50°F/h)

See " 3350 Appliance compute node technical specifications" on page 69.

See " Veritas 5U84 Storage Shelf technical specifications" on page 72.

See "Protocol standards" on page 75.

See "Regulatory, compliance, and certification information" on page 76.

Protocol standards

The following table provides standards with which the Veritas 3350 Appliance and the Veritas 5U84 Primary/Expansion Storage Shelf comply.

Table A-4 Veritas Appliance / Veritas 5U84 Primary/Expansion Storage Shelf standards compliance

Standard	Version
IPMI 2.0	Intelligent Platform Management Interface Specification Second Generation v2.0, Document Revision 1.0
SMBIOS	System Management BIOS (SMBIOS) Reference Specification, Version 2.5
SAS	SAS-3
ACPI	Advanced Configuration and Power Interface Specification, Revision 3.0, September 2
IP	RFC0791: Internet Protocol
PCIe	PCIe 3.0

See " 3350 Appliance compute node technical specifications" on page 69.

See " Veritas 5U84 Storage Shelf technical specifications" on page 72.

See "Environmental specifications" on page 75.

See "Regulatory, compliance, and certification information" on page 76.

Regulatory, compliance, and certification information

The following sections give information about the product regulations and compliance.

WARNING

To ensure regulatory compliance, you must adhere to the assembly instructions in this guide to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components that are specified in this guide. Use of other products or components may void the regulatory approvals of the product. The result is noncompliance with product regulations in the region in which the product is sold.

Before computer integration, ensure that the power supply and other modules and devices have passed appropriate regulatory compliance testing and certification. This process helps to ensure compliance with your local regional rules and regulations. The final configuration of your appliance product may require additional compliance testing.

This product is an FCC Class A device. Integration of it into a Class B system does not result in a Class B device.

Product regulatory compliance

The Access Appliance appliance, when correctly integrated per this guide, complies with the following safety and electromagnetic compatibility (EMC) regulations.

Intended Application - This product was evaluated as Information Technology Equipment (ITE), which may be installed in offices, schools, computer rooms, and similar commercial type locations. The suitability of this product for other product categories and environments, other than an ITE application, may require further evaluation. Other product categories and environments may include medical, industrial, telecommunications, NEBS, residential, alarm systems, and test equipment.

Product safety compliance

The following is a list of product safety compliance norms for different countries:

- UL60950 - CSA 60950 (USA / Canada)
- EN60950 (Europe)
- IEC60950 (International)
- CB Certificate & Report, IEC60950 (report to include all country national deviations)
- EN 62368-1:2014 + AC:2015
- EU Directive: Low Voltage 2014/35/EU
- IRAM Certification (Argentina)
- GB4943- CNCA Certification (China)

Product EMC Compliance - Class A Compliance

The following is a list of EMC compliance norms for different countries:

- EU Directive: EMC 2014/30/EU
- EN 55032:2015 +A11:2020

- EN 55024:2010
- EN 61000-3-2:2014
- EN 61000-3-3:2013
- FCC /ICES-003 - Emissions (USA/Canada) Verification
- VCCI Emissions (Japan)
- AS/NZS 3548 Emissions (Australia / New Zealand)
- BSMI CNS13438 Emissions (Taiwan)
- GB 9254 - CNCA Certification (China)
- GB 17625 - (Harmonics) CNCA Certification (China)

Product ecology compliance

Use of banned substances are restricted in accordance with world-wide regulatory requirements. A Material Declaration Data Sheet is available.

Restrictions include quantity limitations on the following:

- Quantity limit of 0.1% by mass (1000 PPM) for: Lead, Mercury, Hexavalent Chromium, Polybrominated Biphenyls Diphenyl-Ethers (PBB/PBDE)
- Quantity limit of 0.01% by mass (100 PPM) for: Cadmium
- California Code of Regulations, Title 22, Division 4.5, Chapter 33: Best Management Practices for Perchlorate Materials
- China - Restriction of Hazardous Substances (China RoHS)
- WEEE Directive (Europe)
- Packaging Directive (Europe)

Certifications / Registrations / Declarations

The following is a list of the required certifications, registrations, and declarations:

- NRTL Certification (US/Canada)
- CE Declaration of Conformity (CENELEC Europe)
- FCC/ICES-003 Class A Attestation (USA/Canada)
- VCCI Certification (Japan)
- C-Tick Declaration of Conformity (Australia)
- MED Declaration of Conformity (New Zealand)

- BSMI Certification (Taiwan)
- IRAM Certification (Argentina)
- CNCA CCC Certification (China)
- Ecology Declaration (International)
- China RoHS Environmental Friendly Use Period
- Packaging & Product Recycling Marks

Electromagnetic compatibility notices

The following sections list the compatibility notices for USA, Canada, Europe, Japan, and Taiwan.

FCC Verification Statement (USA)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If the equipment is not installed and used in accordance with the instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to a radio or a television reception (can be determined by turning the equipment off and on), the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit other than the one to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help. Any changes or modifications not expressly approved by the grantee of this device can void the user's authority to operate the equipment. The customer is responsible to ensure compliance of the modified product. Only peripherals (computer input or output devices, terminals, printers, etc.) that comply with FCC Class A or B limits may be attached to this product. Operation with noncompliant peripherals is likely to result in interference to radio and TV reception. All cables that are

used to connect to peripherals must be shielded and grounded. Operation with regulatory and compliance information 65 Electromagnetic compatibility notices the cables that are connected to peripherals that are not shielded and grounded may result in interference to radio and TV reception.

ICES-003 (Canada)

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Apparelis Numériques", NMB-003 édictee par le Ministre Canadian des Communications.

English translation of the notice above:

This digital apparatus does not exceed the Class A limits for radio noise emissions from the digital apparatus that is set out in the interference-causing equipment standard entitled: "Digital Apparatus," ICES-003 of the Canadian Department of Communications.

CE Declaration of Conformity (Europe)

This product has been tested in accordance to, and complies with the Low Voltage Directive (73/23/EEC) and EMC Directive (89/336/EEC). The product has been marked with the CE Mark to illustrate its compliance.

VCCI (Japan)

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) from Information Technology Equipment. If the product is used near a radio or a television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

BSMI (Taiwan)

The BSMI Certification Marking and EMC warning label is located on the outside rear area of the product.

Index

Symbols

5U84 Expansion Storage Shelf
- about 31
- control panel 47
  - control panel functions 48
- drawer Sideplane hot swap LED indicators 45
- drawer Sideplane Status panels 43
- Expansion I/O modules 55
  - components and locations 56
- printed circuit board (PCB) assembly 41
- rear components 48
  - component locations 50
- technical specifications 72

5U84 Expansion Storage Shelf serial number location 12

5U84 Primary Storage Shelf
- about 31
- control panel 47
  - control panel functions 48
- cooling module components 58
- cooling modules 58
  - component locations 59
- drawer Sideplane hot swap LED indicators 45
- drawer Sideplane Status panels 43
- printed circuit board (PCB) assembly 41
- RAID controller 51
  - components and locations 51
- rear components 48
  - component locations 49
- technical specifications 72

5U84 Primary Storage Shelf serial number location 12

5U84 Storage Shelf Power Supply Units (PSU) 59
- component locations 60

5U84 Storage Shelves
- about 31
- core components 31
- disk drive drawers 35
- Disk Drive In Carrier (DDIC) modules 38
  - components and locations 40
- disk drive slot numbering 35
- plug-in modules 31

5U84 Storage Shelves *(continued)*
- printed circuit board (PCB) assembly
  - Baseplane cards 41
  - Sideplane cards 41
- storage options 33
- supported RAID levels 31

A

appliance
- power button LED 21
- system memory configuration 8, 69

C

Cable connection types
- Direct-attach / Twinaxial 24
- fiber optic 24

cables
- multi-mode fiber optic
  - description 64
- network
  - description 64
- power
  - description 61
- SAS-3
  - description 65

Compute node
- control panel 15
  - Power button LED states 21
  - system Status LED indicator 17
- disk drive LED indicators 14
- disk drive LEDs 14
- front panel USB port 15
- rear panel
  - features and connectors 21

compute node serial number location 12

Control panel
- 5U84 Expansion Storage Shelf 47
  - control panel functions 48
- 5U84 Primary Storage Shelf 47
  - control panel functions 48

Control panel *(continued)*
compute node 15
power button LED states 21
system LED descriptions 15
system Status LED indicator 17

D

Disk drive drawers
5U84 Storage Shelves 35
Disk Drive In Carrier (DDIC) modules
5U84 Storage Shelves 38
components and locations 40
disk drive LED indicators
compute node 14
disk drive LEDs
compute node indicators 14
Disk drive slot numbering
5U84 Storage Shelves 35
Drawer Sideplane hot swap LED indicators
5U84 Expansion Storage Shelf 45
LED indicator statuses 46
5U84 Primary Storage Shelf 45
LED indicator statuses 46

E

Environmental specifications 75
Ethernet ports 26
Expansion I/O modules
5U84 Expansion Storage Shelf 55
components and locations 56
Veritas 5U84 Expansion Storage Shelf
LED location and conditions 56

I

I/O configurations
standard available options 23
I/O ports
on-board 24
PCI-based 24
total number of 24

L

LED location and conditions
Expansion I/O modules
Veritas 5U84 Expansion Storage Shelf 56

N

Network interface port locations and speeds 26

P

PCIe-based slot configurations
standard available configurations 23
power button LED
appliance 21
descriptions 21
Power button LED states
compute node
control panel 21
Power Supply Units
5U84 Storage Shelf 59
5U84 Storage Shelf Power Supply Units (PSU)
component locations 60
Printed circuit board (PCB) assembly
5U84 Storage Shelves
Baseplane cards 41
components 41
Sideplane cards 41

R

RAID controller 51
RAID levels
supported 31
Rear panel
5U84 Expansion Storage Shelf
components 48
5U84 Primary Storage Shelf
components 48
compute node
features and connectors 21

S

SAS Activity LED location and conditions
Expansion I/O modules
Veritas 5U84 Expansion Storage Shelf 57
serial number locations
5U84 Expansion Storage Shelf 12
5U84 Primary Storage Shelf 12
compute node 12
Sideplane Status panels
5U84 Storage Shelves 43
descriptions 44
locations 43
statuses 45

Status LED indicator
compute node control panel 17

T

Technical specifications
Veritas 5U84 Storage Shelf 72
technical specifications
Access 3350 Appliance compute node 69

U

USB port
compute node front panel location 15

V

Veritas 5U84 Expansion Storage Shelf
Expansion I/O modules
LED location and conditions 56
SAS Activity LED location and conditions 57

February 2020

Declaration of Compliance with EU-Directive 2015/863/EU (RoHS III)

The Restriction of Hazardous Substances (RoHS) Directive (2002/95/EC, “RoHS 1”) was adopted in February 2003 by the European Union, and took effect on July 1, 2006. This directive and its subsequent RoHS-Recast, RoHS 2011/65/EU (RoHS 2) imposed threshold limits (with exemptions) for six hazardous materials commonly used in Electronic and Electrical Equipment (“EEE”).

On March 31, 2015, the EU Commission published Directive (EU) 2015/863, adding four phthalates to Annex II of the RoHS directive. As of July 22, 2019, phthalates DEHP, BBP, DBP and Diisobutyl phthalate (DiBP) are restricted under RoHS for EEE, bringing the current number of restricted substances to ten:

- Lead (0,1 %)
- Mercury (0,1 %)
- Cadmium (0,01 %)
- Hexavalent chromium (0,1 %)
- Polybrominated biphenyls (PBB) (0,1 %)
- Polybrominated diphenyl ethers (PBDE) (0,1 %)
- Bis(2-ethylhexyl) phthalate (DEHP) (0,1 %)
- Butyl benzyl phthalate (BBP) (0,1 %)
- Dibutyl phthalate (DBP) (0,1 %)
- Diisobutyl phthalate (DIBP) (0,1 %)

Starting from 22 July 2019, electrical and electronic equipment on the EU market will have to comply with the new requirements. The enforcement date for medical devices and monitoring and control instruments is 22 July 2021.

DEHP can be found in insulation for cables, capacitors and ceramics for electronics. BBP is possibly contained in PVC sheets, sealants and adhesives of electrical and electronic equipment (EEE). DBP can be part of components of EEE such as cables, plugs and shock absorbers. DIBP has very similar application properties to DBP and may be used to substitute DBP in most of its applications. Therefore, restriction of DIBP in electrical and electronic products under RoHS is recommended to be tied to that of the other three phthalates.

Starting from 2019, to the best of Veritas´ knowledge, no products sold by Veritas contain any of these 4 phthalates above 0.1% in homogeneous materials.

Reference: Commission Delegated Directive (EU) 2015/683 amending Annex II to Directive 2011/65/EU of the European Parliament and of the Council as regards the List of Restricted Substances http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_137_R_0003&from=EN

February 2020

SUPPLIER & MATERIAL CONFIDENCE ASSESSMENT

Veritas follows the BS EN 50581:2012 standard (Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances).

When selecting new suppliers, we only work with high quality/trustworthy suppliers.

We work with our suppliers to risk assess on which components we can rely on our suppliers' declarations or in which ones we need to decide we need to test the components.

- We carry out a risk assessment of our suppliers.

- Depending on the outcome of the assessment we decide whether we need:
  - Supplier Declaration of compliance and/or contractual agreements AND/OR
  - Material Declarations AND/OR
  - Analytical test results

VERITAS

NetBackup Flex Appliance Security

Elevated data protection.

White Paper | December 2023

Introduction

Data security is as important as data availability. The Mid-Year Update to the 2023 SonicWall Cyber Threat Report shows 2.7 billion malware and 140 million ransomware attacks. Cryptojacking attacks grew by 399% reaching 323 million by the end of June 2023. According to Cybersecurity Ventures, by 2031 a business will fall victim to a ransomware attack every two seconds—and the attacks will cost more than $265 billion annually.

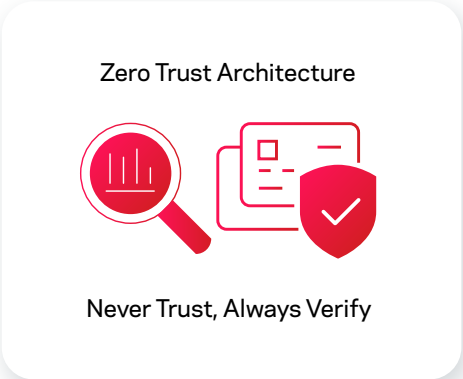
Successful, high-profile cyberattacks frequently resulting in multi-million dollar losses have raised the importance of secure and reliable data protection. Backup as a last resort for organizations' data recovery has also become the main target for cybercriminals.

This document describes security measures and enhancements implemented on Veritas NetBackup Flex appliances. The objective is to emphasize Flex appliances' high security features and how they benefit customers in guarding backup data and the data protection environment against ransomware, cryptojacking, and intrusion attacks.

Flex Appliance Security

Overview

The Zero Trust security model or architecture based on the never trust, always verify principle has been the primary design guideline for Flex appliances from their inception. With Zero Trust by default, users, devices, services, and processes are not trusted and require identity verification along with the least privilege resource access. The Zero Trust model is instantiated on Flex appliances on multiple levels, starting at restraining system access, and culminating with blocking access to the data destruction operations.



The main cyber resiliency barriers may be grouped into the following objectives:

- Restricting system network access
- Preventing unauthorized user login
- Limiting user and process permissions at the operating system and applications
- Restricting access to destructive storage operations

As each barrier is penetrated, the appliance security controls become more restrictive at every stage to reduce the risk of damage to the backup data. For example, if a bad actor gains network system access due to an incorrectly configured firewall and lax network access controls, the appliance—and consequently backup data—is still secure, since the unauthorized user login controls are in place to prevent cybercriminals from logging in.

We will examine each control in greater detail and describe its advantages from the security perspective and the corresponding benefits. See Figure 1 for an outline of appliance security measures.

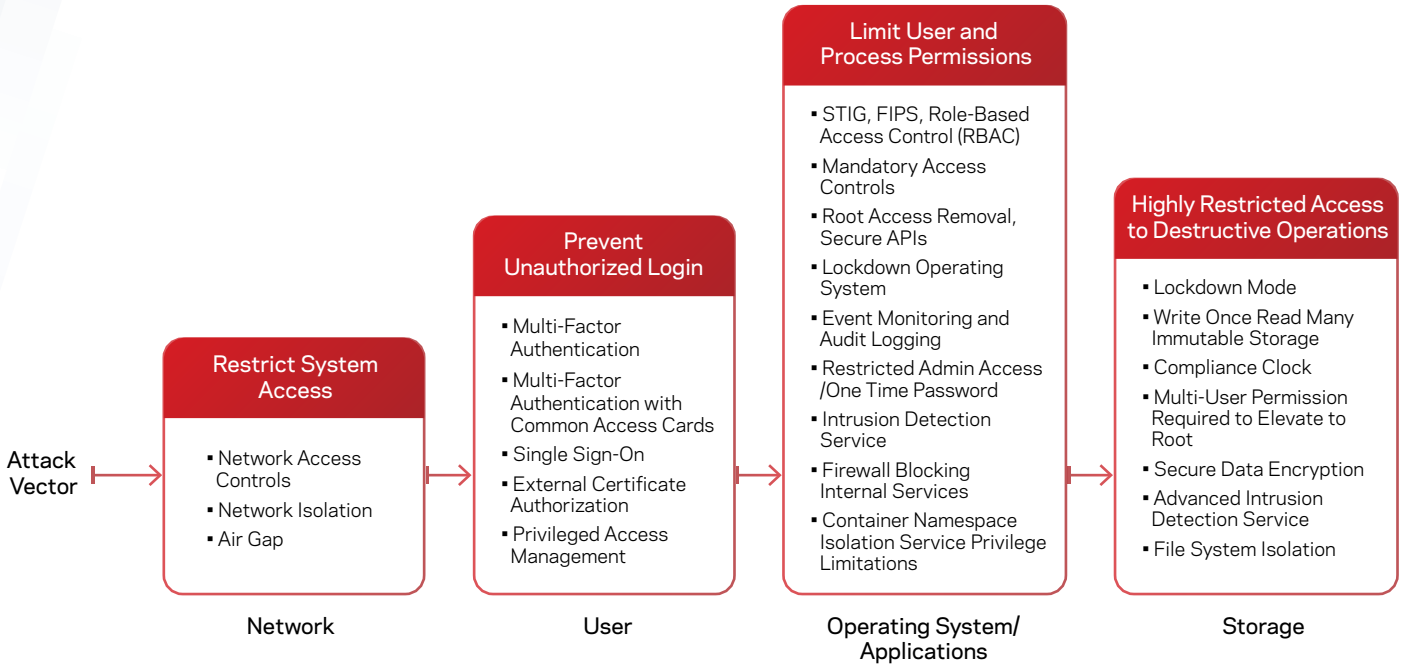


Figure 1. Flex Appliance Security Barriers

Restricting System Access

Modern computers provide multiple potential system entry points that can be exploited by hackers. Flex appliances restrict system access using the following techniques:

- Network Access Controls
  Administrators can manage appliance access by creating separate lists of IP addresses allowed to connect using Secure Shell (SSH) and HTTPS protocols. Connection requests from IP addresses and subnets not listed in network access controls are automatically rejected. For increased security, the default SSH port 22 can be modified.
- Network Isolation
  All applications running on Flex appliances, including NetBackup primary and media servers, are deployed as containers and are network segregated. Appliances deploy MACVLAN type VEPA technology, where the network traffic between the containers is transmitted over the physical interface even if all instances (containers) are connected to the same NIC. This network implementation prevents direct inter-container communication and container-to-container attacks.
- Air Gap
  One of the security features of NetBackup is its ability to maintain an isolated copy of backup data, referred to as an air-gapped copy. This air-gapped copy is in an isolated recovery environment (IRE) that is created on a write once, read many (WORM) storage device. The network access to data in an isolated recovery environment is available only during the replication window, otherwise the air-gapped copy is protected against malware and ransomware attacks.

Preventing Unauthorized Login

Once system access is gained, user authentication (login) is required. Multiple authentication options are available to prevent unauthorized appliance login:

- Multi-factor Authentication
  Multi-factor authentication requires at least two factors (elements) of authentication before user is granted access to the resources. Multi-factor authentication on Flex appliances can be configured by individual users however, once enforcement is activated multi-factor authentication cannot be disabled.

- Multi-Factor Authentication with Common Access Cards (CAC)
  Common access cards provide two-factor authentication, where access to the resources is granted upon the card possession, as well as knowledge of the personal identification number (PIN).
- External Certificate Authority-Issued X.509 Certificate
  By default, Flex appliances use a self-signed certificate. Users may be able to gain appliance access by importing the X.509 certificate issued by an external certificate authority. Only users in possession of the X.509 certificate will be allowed to log in. This certificate is different from the NetBackup primary and media servers.
- Single Sign-On
  Single sign-on (SSO) is supported, however only identity providers using Active Directory or LDAP are supported with SAML 2.0-compliant identity providers.
- Privileged Access Management
  Flex appliances support external password management, such as CyberArk Privileged Access Management, to enforce password rotation policy and privileged session activity and monitoring.
- Intrusion Protection System
  The Intrusion Protection System analyzes system and network activity and logs any unauthorized access attempts.

Limit User and Process Permissions

If bad actors manage to successfully gain access and login to the appliance, additional restrictions implemented compliant with well-defined security standards provide further protection for the backup data and prevent system damage.

- Security Technical Implementation Guides (STIG) Compliance
  STIG is a cybersecurity configuration standard and methodology for securing protocols. Flex appliances are STIG compliant at the operating system (software and firmware) and appliance management level by using the STIG template to meet security requirements per the Defense Information Systems Agency (DISA) profile. Some examples of Flex appliance Security Technical Guides implemented for operating system hardening include:
  - Audit logging of cluster and appliance events—operations that are initiated by users such as login, add node, and configuration changes
  - Auditing is enabled for low-level operations such as operating system commands and system calls
  - Ctrl-Alt-Del (soft) reboot is disabled
  - SSH root login is disabled
  - Interactive/login session idle timeout enforcement
  - Limited number of concurrent login sessions
  - Forced password changes during initial configuration (default password change)
  - Logging of incorrect login attempts
  - Appliance console lock after three incorrect login attempts
  - Customizable password policies—the ability to set customized password policy, including the option to use STIGs for validation
  - Restricted access to GRUB (boot loader) menu
  - Conformance to the Federal Information Processing Standards (FIPS) 140-2
- Federal Information Processing Standards (FIPS)
  FIPS are National Institute of Standards and Technology standards for computer security and interoperability. Flex appliance operating system, platform software, and the NetBackup container conform to FIPS 140-2. Flex also takes advantage of the Security Enhanced Linux (SELinux) framework to create and enable proprietary security policies that conform with STIG guidelines (DISA RHEL7 profile) to further harden the operating system from malicious attacks.

- Role-Based Access Control (RBAC)

  Role-based access control is a security control mechanism where system and resource access are managed based on roles. Flex appliance has three roles: Super administrator, Administrator, and Security administrator. The Administrator role is assigned to all users, but only users with the Security administrator role can manage users and security of the appliance. The Super administrator role is assigned to the default user admin. This role and user cannot be changed.

- Mandatory Access Control

  Mandatory access control constrains processes and threads from accessing and taking certain actions on system resources, such as shared memory segments, file system objects, network ports, and IO devices. The Flex operating system explicitly denies access to all resources—only programs and activities specifically requiring resource access are granted the right to use them, regardless of their system privileges.

- Root Access Removal

  The Linux security model allows the root to bypass security checks; however, the Flex appliance operating system eliminates console root account access. Only the hostadmin user is allowed to log in via SSH to the compute nodes.

- Secure APIs

  Veritas provides a set of secure rest API calls to programmatically manage and monitor the appliances. API access tokens are required for appliance access. The Administrator]can generate a Metrics token for the third-party analytics application, and a Support token for Veritas technical support personnel, to grant permissions to create, download, and clean up log packages. Appliance administration via API also requires credentials to create an X-AUTH-TOKEN for any management tasks. API executions are logged.

- Lockdown Operating System

  Flex appliances can lockdown the operating system. Once the operating system is locked down, modification to operating system services, network, and device drivers is not permitted. The lockdown mode prevents unauthorized changes, even in situations where appliance authorization has been compromised (stolen credentials). For the emergency operations, a one-time password is required. The one-time password can be obtained from Veritas technical support to temporarily unlock the appliance.

- Event Monitoring and Audit Logging

  Flex appliances monitor and analyze system events. All CLI commands and API executions are logged in a separate file and forwarded to the syslog for possible security incident investigation. Appliance system and audit logs can be forwarded to an external log management server. For improved security, TLS log transmission is also available.

- Restricted Admin Access/One-Time Password

  When in lockdown mode, the user admin (Super administrator) has restricted access which does not allow operating system and volume modifications such as deletion, mounting, and unmounting. Installation and uninstallation of software packages is also forbidden. In cases where restricted actions are required, dual authentication and participation from Veritas technical support is necessary to generate a one-time password for access to the appliance.

  Appliance hostadmin and application (NetBackup) appadmin users are forced to change the initial default password upon the first successful login.

- Intrusion Detection

  NetBackup Flex helps protect the system from an attack, misuse, or compromise with its built-in intrusion detection system (IDS), including an advanced intrusion detection environment (AIDE) and an intrusion prevention system (IPS). Intrusion detection isolates each application by allowing access only to assigned resources and processes.

- Firewall Blocking Internal Services

  The built-in firewall blocks all access except ports required for backup and management. All other internal services are blocked.

- Container Namespace Isolation and Service Privilege Limitations

  Flex appliances feature a highly secure, hardened Linux-based VxOS operating system that serves as a hosting platform for containerized services such as NetBackup, appliance management, and a metrics collection time series database, among others.

Containers are inherently more secure than traditionally-executed applications because of the separate resource allocation and logically independent configuration. Applications are packaged in binary bundles which undergo checksum verification before the execution. This approach assures immutability of the binaries and applications included in the container image. The logical independence is derived from the separation of various NetBackup functions (services) into different containers that can only access their own discrete resources. Moreover, NetBackup services are also separated from the backup images stored in WORM storage.

As mentioned earlier, the MACVLAN type VEPA architecture provides containers with network segregation. Sharing the host network with containers is also blocked to prevent snooping on communication between the services.

Containers are also assigned limited-service privileges to define intra-container executables and which system calls are allowed without the need for elevated system privileges.

Highly Restricted Access to Destructive Operations

For sensitive data, additional controls may be configured, virtually eliminating access to damaging operations such as volume formatting and deletion. Entry to hardware-based utilities is also protected. These controls are organized into lockdown modes. Different lockdown modes and corresponding restrictions are described below, along with additional security features:

- Lockdown Mode
  Flex appliance lockdown mode offers additional security levels to protect your appliance and data—it is a core component of the appliance immutable architecture. Lockdown mode sets the appliance into a heightened security level to protect data and the storage infrastructure. When in lockdown mode:
  - Administrators cannot make changes to the operating system, operating system services, and hardware device drivers.
  - WORM storage instances can be created only in lockdown mode. Any data written to WORM storage is immutable, which means it is marked as read only and cannot be modified, corrupted, or encrypted. Moreover, the data on WORM storage is also indelible, making it impossible to delete before the retention period expires.

  Flex appliance supports the following lockdown modes:

- Normal Mode
  This mode is the default mode of the appliance. Normal mode does not support WORM storage.
- Enterprise Mode
  - You can create WORM storage instances and delete them, including volumes with existing data
  - Any administrator can delete WORM storage instances if there is no immutable data. However, only the default admin user can delete them if immutable data is present
  - When you delete a WORM storage instance as the default admin user, the instance can be running or stopped; when you delete a WORM instance as any other user, the instance must be running so that the system can verify that there is no immutable data present
  - To change from enterprise mode to normal mode, you must first delete all WORM storage instances
- Compliance Mode
  - You can create WORM storage instances; you can delete the instances only if there is no immutable data present
  - Any administrator can delete WORM storage instances if there is no immutable data
  - When you delete a WORM storage instance, the instance must be running so that the system can verify that there is no immutable data present
  - To change from compliance mode to enterprise mode or normal mode, you must first wait for all data on the WORM storage instances to expire and then delete the instances

See Table 1 for a summary of possible actions based on the lockdown mode.

Action	Normal Mode	Enterprise Mode	Compliance Mode
Create WORM Storage	No	Yes	Yes
Delete WORM Storage—No Data	N/A	Yes	Yes
Delete WORM Storage—Data Present	N/A	Yes	No
Storage Reset	Yes	No	No

Table 1. Lockdown Modes

- WORM Immutable Storage
  WORM storage provides data immutability and indelibility. The primary server sets up immutability controls such as mandatory data retention policy. WORM storage is available only when appliance is in lockdown mode.
- Compliance Clock
  The central attribute of WORM is the ability to accurately measure elapsed time to ensure minimum and maximum data retention duration. The immutable clock is independent of the operating system time, and the Network Time Protocol (NTP) is a function of the compliance clock. The compliance clock is tamper-proof—even the NetBackup administrator does not have the ability to modify it.
- Multi-User Permission Required to Elevate to root
  Before root access is granted to the shell, a separate password from a different user—external to the appliance—is required.
- Secure Data Encryption
  Data selected for backup, restore, and duplication, as well as corresponding metadata are encrypted over a secure TLC channel while in transit between NetBackup entities (primary and media servers). Encryption for data at rest is also available, including client-side, multi-server deduplication pool, cloud, tape drive, and AdvancedDisk destinations.
- Advanced Intrusion Detection Service
  As part of STIG rules, the Advanced Intrusion Detection Service keeps track of file systems and generates alerts if any new software is deployed, or if any changes are made to the operating system files. This feature provides enhanced visibility into important user and system actions to ensure a valid and complete audit trail that addresses compliance regulations such as Payment Card Industry as a compensating control.
- File System Isolation
  Access to the root filesystem is restricted to read only operations—even for the admin account—to prevent accidental or malicious damage. Host-level services are also blocked from accessing the container file systems. Additionally, dedicated filesystems mounted with security context are available for container-exclusive access, where file system sharing is not permitted. This makes each file system visible and accessible only by a single, specific container.

Security Updates

The dynamic nature of the security landscape, with discoveries of new vulnerabilities and more sophisticated attack techniques, requires frequent and regular appliance updates. Veritas is committed to delivering hotfixes for critical exploitable vulnerabilities within 30 days or as mandated by the Cybersecurity Information Security Agency. Maintenance releases are to be delivered about every 90 days, with fixes for medium, high, and critical vulnerabilities.

Security Meter

To simplify the process of securing the platform, Flex appliances include a Security Meter, which is a tachometer-style widget. The Security Meter evaluates the current state and recommends required actions to change the protection ranking from Good to Excellent. Some settings are enabled by default and cannot be modified, whereas recommendations are linked to the appropriate configuration section where they can be easily changed. The Security Meter is available only to the Super administrator (admin) user.

Summary

Veritas invests significant research and engineering resources in the development of Flex appliances to deliver a stable, reliable, and highly secure data protection solution. With each product release and regular product updates, new security features are added, and existing ones are enhanced to lower the risk ofcurrent and future threats. This highly secure platform, combined with the unbeatable NetBackup reputation, makes for an ideal solution for customers seeking an easy-to-deploy, flexible, scalable, and secure data protection environment.

References

NetBackup and Veritas Appliances Hardening Guide

Veritas Flex Appliance Getting Started and Administration Guide

About Veritas

Veritas Technologies is the leader in secure multi-cloud data management. Over 80,000 customers—including 91% of the Fortune 100—rely on Veritas to help ensure the protection, recoverability and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems and 1,400+ storage targets through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on X at @veritastechllc.

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1108 12/23