Updated June 2021

Product type

Storage Shelf sold as part of a storage system

Manufacturer's name, registered trade name, and registered address

NetApp
NetApp, Inc.
1395 Crossman Ave.
Sunnyvale, CA 94089
United States
+1 408-822-6000

Product model number	Marketing model Number
NAJ-1801	NS224, NE224

First year of manufacture

2019

PSU efficiency

Load percentage	DPS-1600AB-18 PSU efficiency
10%	89.50%
20%	92.93%
50%	94.37%
100%	92.71%
Average efficiency	93.84%
Power Factor at 50% load	0.980

Declared ASHRAE operating condition class

ASHRAE rating	A4
Allowable operating temperature range	5 to 45 degrees C
Recommended operating range	18 to 27 degrees C
Allowable operating relative humidity	-12ºC DP and 8% to 24ºC DP and 90%
Recommended operating relative humidity	-9ºC DP to 15ºC DP and 60%
Maximum Dew Po9int	24
Maximum rate of change (ºC/hr)	5/20

Material ease of disassembly for repair or reuse

E-Series: https://docs.netapp.com/ess-11/index.jsp in the System maintenance tab

Neodymium in HDDs

All 10K RPM and 15K RPM drives have less than 5 g
All 7200 RPM drives have between 5g and 25g

Cobalt in Li-Ion Batteries

All Li-Ion Cells have less than 5g
All Li-Ion Battery Packs have between 5g and 25g

Secure data deletion information: E-series

Storage Shelf must be installed as part of a storage system.

E-series secure data deletion capability is provided by a Python script which will issue commands appropriate for the drives in the array configuration to eliminate all user data.
Minimum SANtricity OS (controller software) level required is 11.70.1.

The script can be downloaded at this location:
https://mysupport.netapp.com/site/products/all/details/eseries-santricity/downloads-tab/download/62736/SecDel2020/downloads

To run the script, a host (Linux or Windows) is required, with the following connectivity and components:

- Network connectivity to the array
- Python 3.6 with the 'requests' library

Secure data deletion information: FAS and AFF

Storage Shelf must be installed as part of a storage system.

Security Hardening Guide for NetApp ONTAP 9 (page 18)

Starting with ONTAP 9.4, you can use the secure-purge feature with advanced privilege to nondisruptively "scrub" data on NVE-enabled volumes. Scrubbing data on an encrypted volume ensures that it cannot be recovered from the physical media. The following command securely purges the deleted files on vol1 on SVM vs1: cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1 Starting with ONTAP 9.7, NAE and NVE are enabled by default. If the VE license is in place, either OKM or external key managers are configured, and NSE is not used, then NAE and NVE are enabled by default. NAE volumes are created by default on NAE aggregates, and NVE volumes are created by default on non-NAE aggregates. This can be overridden by entering the following command: cluster1::*> options -option-name encryption.data_at_rest_encryption.disable_by_default true For more information about NSE, NVE, NAE, OKM, and external KMIP servers, see NetApp Encryption Power Guide in the ONTAP 9 Documentation Center.

Clean up data spills quickly with NetApp secure_purge - analst review