LENOVO

DASH GUIDE

ThinkStation

Contents

1. THINKSTATION DASH SUPPORT

1.1 Introduction

Dash (desktop and mobile architecture for system hardware) is a set of specifications developed by dmtf, which aims to provide open standards based web service management for desktop and mobile client systems. Dash is a comprehensive framework that provides a new generation of standards to protect the security of out of band and remote management of desktop and mobile systems in multi vendor, distributed enterprise environments. Dash uses the same tools, syntax, semantics, and interfaces across the product line (traditional desktop systems, mobile and laptop computers, blade PCs, and thin clients).

For more information, please refer to the following links:
https://www.dmtf.org/standards/dash

1.2 Profile List

BIOS Management Profile	DSP1061	
Boot Control Profile	DSP1012	Only support one time boot
CPU Profile	DSP1022	
DHCP Client Profile	DSP1037	
DNS Client Profile	DSP1038	
Ethernet Port Profile	DSP1014	
Host LAN Network Port Profile	DSP1035	
Power State Management Profile	DSP1027	
Sensors Profile	DSP1009	
SSH Service Profile	DSP1017	
KVM Redirection Profile	DSP1076	
System Memory Profile	DSP1026	
Software Update Profile	DSP1025	Only support Update onboard LAN FW
Text Console Redirection	DSP1024	
IP Interface Profile	DSP1036	
Physical Asset Profile	DSP1011	
Service Processor Profile	DSP1018	
Telnet Service Profile	DSP1016	

IP Configuration Profile	DSP1116	
PCI Device Profile	DSP1075	
Record Log Profile	DSP1010	
OS Status Profile	DSP1029	
Indication Profile	DSP1054	
Watchdog Profile	DSP1040	
Physical Computer System View Profile	DSP1108	
Software Inventory Profile	DSP1023	

1.3 Support OS

Microsoft Windows 10

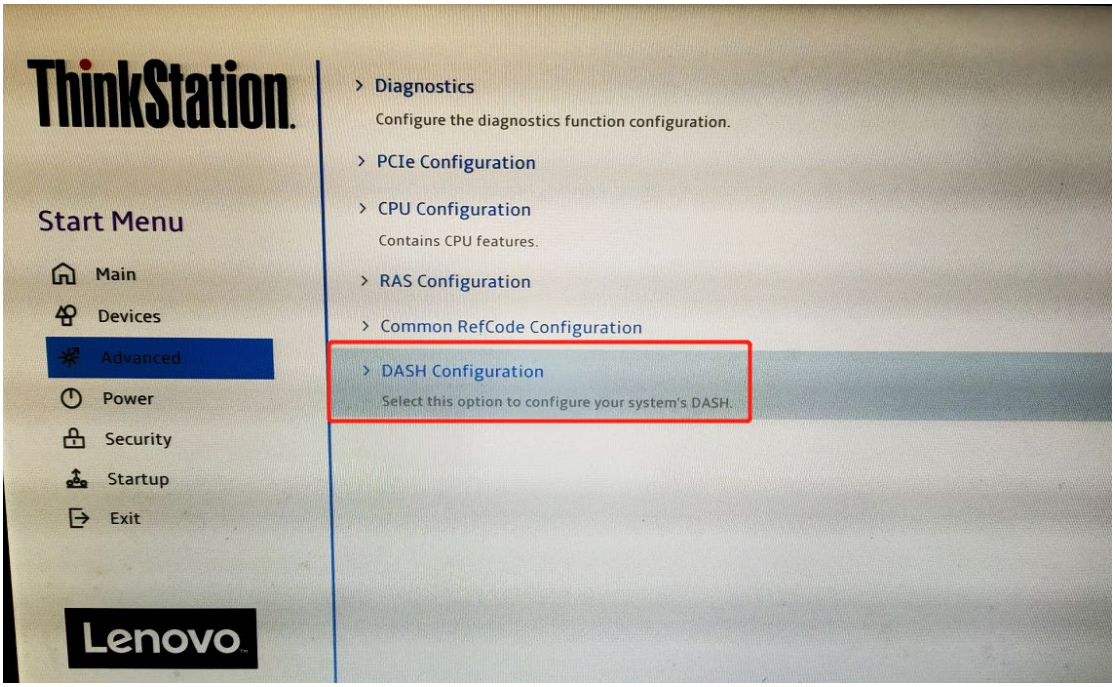
2. Preparation

2.1 Download DASH Tool

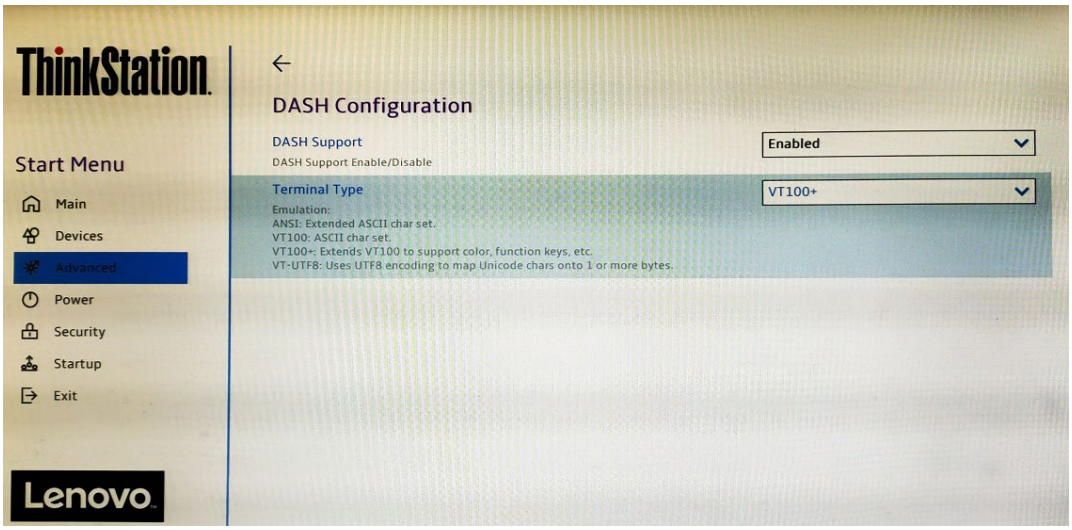
Download the latest DASHCLI from AMD (https://developer.amd.com/tools-for-dmtf-dash/).
Download Lan FW package from Lenovo Web (https://support.lenovo.com/us/en).

2.2 Enable DASH in BIOS

a) Press F1 to enter BIOS setup
b) Advanced->DASH Configuration



c) DASH Support=Enabled (default is Disable)



2.3 Config DASH in WINDOWS

a) Follow "HOW TO CREATE CERTIFICATES FILES" to create .crt and .nopp.key files
b) Run Powershell or CMD as Administrator
c) cd to enters FW package directory
d) AqDashAgent.exe install

```
PS C:\Windows\system32> cd C:\Users\      \Desktop\FWPackage
PS C:\Users\      \Desktop\FWPackage> .\AqDashAgent0.26.exe install
Service 'AqDashSvc' started
Service 'AqDashSvc' installed successfully.
```

e) Config DASH exclusive mode command is:

AqDashConfig.exe exclusive User Password .\crtfile .\keyfile --mac xx:xx:xx:xx:xx:xx --ip xxx.xxx.xxx.xxx

User: is DASH management account

Password: DASH management password

server.crt and server.nopp.key are certificates files that a) step create

In exclusive mode, DASH MAC and IP address are independent, must different with onboard Lan's MAC and IP address

```
PS C:\Users\      \Desktop\FWPackage> .\AqDashConfig0.26.exe exclusive User Password .\server.crt .\server.nopp.key --mac 00:17:B6:00:00:01 --ip 192.168.1.155
Aquantia DASH Configuration Tool v0.12.0 (bundle v0.26.0)
Found 4 ASF power control operations
Found 1 adapter(s):

Selected 'Marvell AQtion 10Gbit Network Adapter' adapter.
[*] DASH successfully configured!
```

f) Config DASH shared mode command is:

AqDashConfig.exe shared User Password .\ crtfile .\ keyfile

User: is DASH management account

Password: DASH management password

server.crt and server.nopp.key are certificates files that a) step create

```
PS C:\Users\      \Desktop\FWPackage> .\AqDashConfig0.26.exe shared User Password .\server.crt .\server.nopp.key
Aquantia DASH Configuration Tool v0.12.0 (bundle v0.26.0)
Found 4 ASF power control operations
Found 1 adapter(s):

Selected 'Marvell AQtion 10Gbit Network Adapter' adapter.
[*] DASH successfully configured!
```

Note: For more detail, please use -h parameter to get the help message.

Note:

Exclusive mode - allows the user/DASH admin to explicitly configure the DASH interface(s) to have unique MAC and IP addresses from the OS equivalents.

- Exclusive provides flexibility, more security(?) but requires a minimum of 2x MAC and 2x IP addresses per host (ip_1=OS NIC interface, ip_2=DASH interface)
- requires marginally more administration during configuration
- an advantage when IT has separate VLANs and or IT asset management networks
- This mode is currently working and supported in latest Marvell software

Shared mode - allows the DASH interface and OS interface, both physical (MAC) and logical (IP) to share a single MAC and IP address.

- This mode has simpler configuration and uses few resources (single IP and single MAC)
- This mode also combines OOB management traffic on the inband OS traffic
- Marvell currently sizing bringing in Shared mode support

2.4 Install Management Console

Install DASHCLI and follow user guide (X:\Program Files (x86)\DASH CLI 3.0\docs) to manage DASH client.

a) DASH CLI Option

Option	Usage	Description
help	help	Display help
version	version	Show DASH CLI version
-h	<host>	Host name or IP address
-p	<port(s)>	Server Port(s)(For discovery more than one ports can be specified separated by commas)
-u	<username>	User Name
-P	<password>	Password
-a	<digest|basic|gss>	Authentication Type [default=digest]
-S	<http|https>	HTTP Scheme [default=http]
-C		Ignore certificate/do not verify certificate (To verify, certificate should be stored in certificate store)
-t	<targetpath>	Target Path
-s	<startip>	Start IP address for discovery (only for discovery)
-e	<endip>	End IP address for discovery (only for discovery)
-T	<timeout>	Timeout in seconds
-v	<1|2>	Verbose Level [1 - More explanation on error or 2-Dump WSMAN data]
-o	<verboseoutput>	Verbose output file to dump wsman data [default is stdout].

b) DASH CLI Commands

Command	Description
help	Display help
version	Show DASHCLI version
enumerate	Enumerate targets
discover	Perform discovery
account	Creates, Deletes and Manages the Account
roles	Manages the Roles
softwareupdate	Update software of the managed element

c) DASH CLI Target

DASH Command	Description
bios	List the BIOS information. Other operations: Set BIOS Attributes. (DSP1061 - BIOS Management Profile)
bootconfig	List the boot configuration information. It is used to

	performs Boot Config operations: Change Boot order, set next boot, set default boot, add new boot configuration or Delete and existing Boot Configuration. (DSP1012 - Boot Control Profile)
computersystem	List the computer system information. It is also used to read Computer System's Power, Processor, Sensor, Software, Asset, Fan, Boot Configuration & User Profiles. It is also used by subcommands to add user, boot config or create Opaque Management Data. (DSP1058 - Base Desktop Mobile)
dhcpclient	List the DHCP Client information. (DSP1037 - DHCP Client Profile)
dnsclient	List the DNS Client information. (DSP1038 - DNS Client Profile)
ethernetport	List the ethernet port information. (DSP1014 - Ethernet Port Profile)
ipinterface	List the IP interface information. (DSP1036 - IP Interface Profile)
kvmredirection	List the KVM Redirection information. It is used to performs KVM operations: Enable, Disable, Connect and Start KVM. (DSP1076 - KVM Redirection Profile)
memory	List the memory information. It is also used to provide information regarding memory's assets. (DSP1026 - System Memory Profile)
networkport	List the network port information. (DSP1035 - Host LAN Network Port Profile)
computersystem power	List the power information. Manage Power states of DASH system. (DSP1027 - Power State Management)
processor	List the processor information. (DSP1022 - CPU Profile)
role	List the role information. It is used to perform Role operations: List Permissions, Set Permissions, Add Permissions, Remove Permissions and Delete. (DSP1039 - Role Based Authorization Profile)
sensor	List the sensor information. (DSP1009 - Sensors Profile)
software	List the software information. It is also used to update the firmware on the system. (DSP1023 - Software Inventory; DSP1025 - Software Update Profile)
textredirection	List the text redirection information. It is used to performs Text Redirection operations: Activate, Disable, Connect, Disconnect and Start. (DSP1024 - Text Console Redirection Profile)

user	List the user information. It is used to perform User operations: Create, Enable, Disable, Assign Role, Remove Role, Change Password and Delete. (DSP1034 - Simple Identity Management Profile 4)
discovery	List the discovery information of DASH System(DSP1034 - Simple Identity Management Profile)

More detail please refer the DASH CLI User Guide.pdf(\DASH CLI 3.0\docs)

3. HOW TO CREATE CERTIFICATES FILES

3.1 Requirements

a) Download and install the latest available OpenSSL package (http://www.openssl.org/).
   i. Ensure openssl.exe is in **%PATH%**
   ii. Ensure that the environment variables has the variable "OPENSSL_CONF"
   OPENSSL_CONF
   C:\Program Files\OpenSSL-Win64\bin\cnf\openssl.cnf

b) Sample **ini** is specified in **3.7**. Save the contents as openssl.ini and modify the file based on your organization requirement.
   Size must be set to 2048. All other sizes are unsupported.
   default_bits = 2048
   i. Per device certificate: A per device certificate can be generated and installed on that particular device (Eg: dash-system.myorg.com). Per device certificate can be generated on alternate names of the systems and also on IP address. For per per device option, under "alt_names" section, add value for key "DNS.1", "DNS.2 and "IP.1". Eg,
   DNS.1 = dash-system.myorg.com <DNS name of DASH system>
   DNS.2 = dash-system
   IP.1 = 10.10.10.100 <IP address of DASH system, e.g. 192.168.1.10>

c) NIC Management Controller specific requirements are mentioned in 3.5

3.2 Create root certificate

A Root certificate is common to the whole organization. It is generated only once and installed in the certificate store.

a) **Create folders & copy openssl.ini**
   mkdir DASHCert
   cd DASHCert
   copy ..\openssl.ini DASHCert

mkdir newcerts private

b) **Create requisite files**

echo 01 > serial

copy /y nul index.txt

c) **Create root certificate(Note:** For 'Common Name', specify the name of the root authority. For instance like 'DASH Root Authority'**)**

openssl genrsa -out private/cakey.pem 1024

openssl req -new -x509 -extensions v3_ca -key private/cakey.pem -out cacert.pem -days 3650 -sha256 -config ./openssl.ini

openssl x509 -in cacert.pem -out DASHCA.crt

3.3 Add root certificate to certificate store on the system with DASH Console

Root certificate must be installed in the certificate store on all console systems where DASH applications like DASH CLI, AMD Management Console and AMPS are installed.

a) Copy DASHCA.crt to DASH Console.

b) Import to certificate store:

i. Right click on DASHCA.crt and select 'Install Certificate'

ii. Select "Local Machine" as Store Location

iii. Click Next and select 'Place all certificates in the following store'

iv. Click Browse and select 'Trusted Root Certification Authorities'

v. Click Next & Finish

3.4 Generate per-device certificate

a) Create certificate signing request

Note: For 'Common Name', specify the generic (Eg: *.myorg.com).

openssl req -new -nodes -out req.pem -sha256 -extensions v3_req -config ./openssl.ini

b) Sign certificate

openssl ca -out cert.pem -extensions v3_req -config ./openssl.ini -infiles req.pem

c) Strip readable text

move cert.pem tmp.pem

openssl x509 -in tmp.pem -out cert.pem

3.5 Import certificate on the DASH System

Executing the commands below will over-write the existing certificate details.

For shared mode use the following command:

AqDashConfig.exe shared admin adminpass cert.pem key.pem

For exclusive mode use the following command:

AqDashConfig.exe exclusive admin adminpass cert.pem key.pem --mac 00:17:B6:10:10:10 --ip 192.168.1.10

3.6 Verification

To verify the certificate installed correctly and DASH HTTPS is working.

Run a DASH CLI https command without -C option. DASH CLI must provide the output without any error.

dashcli -h dash-system.myorg.com -p 664 -S https -a digest -u admin -P adminpass -t computersystem[0] power status

dashcli -h 192.168.1.10 -p 664 -S https -a digest -u admin -P adminpass -t computersystem[0] power status

3.7 Openssl.ini sample

```
# OpenSSL configuration file.
#----Begin----
# Establish working directory.
dir = .

[ ca ]
default_ca = CA_default

[ CA_default ]
serial = $dir/serial
database = $dir/index.txt
new_certs_dir = $dir/newcerts
certificate = $dir/cacert.pem
private_key = $dir/private/cakey.pem
default_days = 3650
default_md = sha256
preserve = no
email_in_dn = no
nameopt = default_ca
certopt = default_ca
policy = policy_match
```

```
[ policy_match ]
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = optional
commonName = supplied
emailAddress = optional

[ req ]
default_bits = 2048
default_keyfile = key.pem
default_md = sha256
string_mask = nombstr
distinguished_name = req_distinguished_name

[ req_distinguished_name ]
# Variable name Prompt string
#---------------------- ---------------------------------
0.organizationName = Organization Name (company)
organizationalUnitName = Organizational Unit Name (department, division)
emailAddress = Email Address
emailAddress_max = 40
localityName = Locality Name (city, district)
stateOrProvinceName = State or Province Name (full name)
countryName = Country Name (2 letter code)
countryName_min = 2
countryName_max = 2
commonName = Common Name (hostname, IP, or your name)
commonName_max = 64
# Default values for the above, for consistency and less typing.
# Variable name Value
#------------------------------ ------------------------------
0.organizationName_default       = MyOrg Inc
organizationalUnitName           = IT
countryName_default              = IN
stateOrProvinceName_default      = KA
localityName_default             = Bangalore
emailAddress_default             = it@myorg.com
organizationalUnitName_default   = IT Department
commonName_default               = *.myorg.com
```

```
[ alt_names ]
# Hostname of target with FQDN can also be entered in the form *.domain.com
DNS.1        = *.myorg.com
#DNS.2       = dash-system.myorg.com
#DNS.3       = dash-system
# IP address can be allowed with the IP Key
#IP.1        = 10.10.10.100


[ v3_ca ]
basicConstraints = CA:TRUE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement,
keyCertSign
subjectAltName = @alt_names

[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement,
keyCertSign
subjectAltName = @alt_names
#----End----
```