	PXE	**SZTP**	**FDO**
Device	BMC preconfigured for PXE boot	BMC preconfigured for PXE boot Device identifcation certificate FQDN of configuration server	FDO Client Root of Trust Key (ROT) Installed in TPM or on file system FQDNs of rendezvous servers public or private Digital proof of ownership (ownership voucher)
DHCP Server **DHCPv6 Server**	IPv4 DHCPv4 Supplies: - Subnet mask (DHCP option 1) - Time Zone Offset (DHCP option 2) - IP address of default gateway (DHCP option 3) - Time Server (DHCP option 4) - IP address of DNS server (DHCP option 6) - IP address of log server (DHCP option 7) - DHCP Lease Time Option (DHCP option 51) - IP address of TFTP server (DHCP option 66) - Name of PXELinux Boot Loader file (DHCP option 67) IPv6 ICMPv6 type 134 Router Advertisement Supplies: - Router Lifetime (used to define default router) - Reachable Time - Retrans Time - MTU - Prefix (network) number DHCPv6 Supplies - Time Zone Offset (DHCP option 17[4491].38) - Time Server (DHCP option 17[4491].37) - IP address of DNS server (DHCP option 23) - IP address of log server (DHCP option 17[4491].34) - DHCP Lease Time Option (DHCP option 51) - IP address of TFTP server (DHCP option 17[4491].32) - Name of PXELinux Boot Loader file (DHCP option 17[4491].33)	IPv4 DHCPv4 Supplies: - Subnet mask (DHCP option 1) - Time Zone Offset (DHCP option 2) - IP address of default gateway (DHCP option 3) - Time Server (DHCP option 4) - IP address of DNS server (DHCP option 6) - IP address of log server (DHCP option 7) - DHCP Lease Time Option (DHCP option 51) IPv6 ICMPv6 type 134 Router Advertisement Supplies: - Router Lifetime (used to define default router) - Reachable Time - Retrans Time - MTU - Prefix (network) number DHCPv6 Supplies - Time Zone Offset (DHCP option 17[4491].38) - Time Server (DHCP option 17[4491].37) - IP address of DNS server (DHCP option 23) - IP address of log server (DHCP option 17[4491].34) - DHCP Lease Time Option (DHCP option 51)	IPv4 DHCPv4 Supplies: - Subnet mask (DHCP option 1) - Time Zone Offset (DHCP option 2) - IP address of default gateway (DHCP option 3) - Time Server (DHCP option 4) - IP address of DNS server (DHCP option 6) - DHCP Lease Time Option (DHCP option 51) IPv6 ICMPv6 type 134 Router Advertisement Supplies: - Router Lifetime (used to define default router) - Reachable Time - Retrans Time - MTU - Prefix (network) number DHCPv6 Supplies - Time Zone Offset (DHCP option 17[4491].38) - Time Server (DHCP option 17[4491].37) - IP address of DNS server (DHCP option 23) - DHCP Lease Time Option (DHCP option 51)
DHCP relay agent	Utilized if the DHCP server is not on that same network as the device requesting boot services	Utilized if the DHCP server is not on that same network as the device requesting boot services	Utilized if the DHCP server is not on that same network as the device requesting boot services
Configuration Server	Not applicable	BootStrap Server Device is preconfigured with a certificate before delivery. The bootstrap server is preconfigured with related device certificates. The device uses the preconfigured certificate to perform two-way authentication and establishes an HTTPS connection with the bootstrap server. In this way, secure data exchange is ensured. Bootstrap server sends information such as the IP address of the deployment file server and files to be downloaded from the deployment server to the device.	Rendezvous Server (public or private) After the device boots up, it ‘calls’ the Rendezvous Server (RV) defined in the FDO client The device identifies itself to the RV and in turn the RV matches the device to its target cloud/platform. The web address for the target cloud/platform is provided to the device. Multiple RV’s can be programmed into the device, including both on-prem and cloud

Deployment File Server	Supplied as a DHCP option Devices uses TFTP to download the PXELinux boot loader image file Alternative tranport protocols can be used, but require switch to iPXE. On some NIC, iPXE is support, if not, iPXE can be changeloaded into the PXE ROM iPXE can also support loading of .PXELinux boot loader, or operate as boot load manager.	Stores the deployment files to be loaded to the device(s) Device uses the preconfigured certificate to perform two-way authentication The deployment file server is preconfigured with related certificates. Device uses HTTPS to securely download Onboarding information , Redirect information, Conveyed information, Owner Certificate, and Ownership Voucher: Onboarding information provides data necessary for a device to bootstrap itself and establish secure connections with other systems. It specifies details about the boot image, an initial configuration the device must commit, and scripts that the device must execute. Redirect information is used to redirect a device to another bootstrap server. The redirect information contains a list of bootstrap servers along with a hostname, an optional port, and an optional trust anchor certificate that the device uses to authenticate the bootstrap server. Conveyed Information contains the required bootstrapping data for the device. It contains either the redirect information or onboarding information to provision the device. Owner certificate is installed on the device with the public key of your organization. The router uses the owner certificate to verify the signature in the conveyed information artifact using the public key that is available in the owner certificate. Ownership voucher is used to identify the owner of the device by verifying the owner certificate that is stored in the device.	Based on the information provided by the RV in the prior stage, the device contacts the cloud/platform. The Device uses its Root of Trust to uniquely identify itself to the cloud/platform and in return the cloud/platform identifies itself as the device owner using the Ownership Voucher. Next, these mutual attestations allow a secured, encrypted tunnel to be created between the device and the cloud/platform The cloud/platform can now download over the encrypted tunnel whatever credentials or software agents are needed for correct device operation and management. The device contacts its management platform, which will manage it for the rest of its lifecycle. FDO lies dormant, although it can be re-awakened in the event of a transfer of ownership of the device e.g. its sale.
DNS Server	Provides mappings between domain names and IP addresses, and resolves the domain name of servers used in the bootstrap process	Provides mappings between domain names and IP addresses, and resolves the domain name of servers used in the bootstrap process	Provides mappings between domain names and IP addresses, and resolves the domain name of servers used in the bootstrap process
Syslog	Uploads user logs recorded during the SZTP process to the network management system (NMS).	Uploads user logs recorded during the SZTP process to the network management system (NMS).	Uploads user logs recorded during the SZTP process to the network management system (NMS).