

PRIVATE ENDPOINT AND ACCESS

1. Implemented Azure Storage Private Endpoint with custom DNS to restrict access to a secure VNet, disabling all public endpoints and verifying private-only blob access:



```
Administrator: Command Prompt

Microsoft Windows [Version 10.0.17763.7558]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ssjuser>nslookup rampartsvault.blob.core.windows.net
Server:      UnKnown
Address:     168.63.129.16

Non-authoritative answer:
Name:        rampartsvault.privatelink.blob.core.windows.net
Address:     10.0.0.6
Aliases:     rampartsvault.blob.core.windows.net
```

2. Update DNS — make sure **rampartsvault.blob.core.windows.net** resolves to the private IP:

Customer Visible FQDNs		
DNS records visible to the customer		
Network Interface	IP addresses	FQDN
▼  priv-endpoint.nic.95154840-447d-....		
▼	10.0.0.5	
		rampartsvault.blob.core.windows.net
Custom DNS records		
To be configured correctly, the following FQDNs are required in your private DNS setup. Learn more 		
FQDN	IP addresses	
rampartsvault.blob.core.windows.net	10.0.0.5	