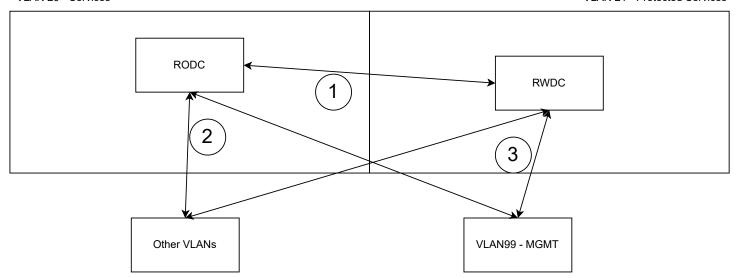
| Identity Services Ecosystem | | | | |
|-----------------------------|----|-----------------|---|--|
| Subsystem Code | ad | Component Codes | Read Write Domain Controller = rwdc Read Only Domain Controller = rodc | |

VLAN 20 - Services VLAN 21 - Protected Services



| Data Flows | | | | |
|------------|--|---|---|--|
| ID | Port/Proto | Description | Controls | |
| 1 | 636/TCP 3269/TCP 88/TCP-UDP 53/TCP-UDP 135/TCP 49152-65535/TCP 445/TCP | Domain Controller Replication, including LDAPS, Global Catalog, Kerberos, DNS, and RPC control and data, and SMB. | Inter-VLAN traffic will be evaluated at the core firewall level, and restricted with Proxmox VM-level firewalls. | |
| 2 | 88/TCP-UDP 53/UDP 445/TCP | Read-Only operations, including Kerberos, DNS lookups, and GPO downloads. | SRV record weights preference all hosts to RODCs for all operations, which refer write operations to WDCs. Site segmentation also ensures DC Locator will locate RODCs first in all cases except for the Protected Services VLAN. Inter-VLAN traffic will be evaluated at the core firewall level and restricted with Proxmox VM-level firewalls. | |
| 3 | 88/TCP-UDP 53/UDP 445/TCP 5986/TCP | Must-Write operations and domain admin functions, including declarative specifications for the domain, users, and groups, as well as adhoc changes included Group Managed Service Accounts (gMSAs). | for all operations, which refer write operations to WDCs. Site segmentation also ensures DC Locator | |

| | Active Directory Site Architecture | | | | |
|----|------------------------------------|--|---------|--|--|
| ID | Site Name | Subnets | DC Type | Description | |
| 1 | Protected-Core | 10.0.21.0/24 | W | Only the protected services get direct access to the WDCs via DC Locator. This IP Space correlates with the Core physical site. | |
| 2 | Primary-Core | 10.0.20.0/24 10.0.40.0/24 10.0.99.0/24 | RO | The Primary set of IP spaces at the Core Physical Site, associated with the RODCs at the Core site. No domain joins on 10.0.99.0/24; only DC Locator | |
| 3 | DMZ-Core | 10.0.30.0/24 | RO | The DMZ at the Core physical site. | |

| | Site Links | | | | |
|----|----------------|--------------|----------------|---|--|
| ID | Site1 | Site2 | Directionality | Description | |
| 1 | Protected-Core | Primary-Core | Bi-Directional | Always on, cost-biased towards RODCs, and not schedule limited. Sites are physically at the same location, so bandwidth/latency isn't a concern | |
| 2 | | | | | |
| | | | | | |

| | Must-Write Use Cases | | | | |
|----|----------------------|---------------------------------------|---|--|--|
| ID | Application | Function | Description | | |
| 1 | General | Domain Joins | Domain Joins possible from any subnet in the domain; will hit the RODC first before getting referred to the RWDC. | | |
| 2 | General | DNS Updates | DHCP hosts can update their own DNS records; will hit the RODC first before getting referred to the RWDC. | | |
| 3 | General | gMSA | Group Managed Service Accounts (gMSAs) are service accounts that can manage their own password, removing the need for a human to set a potentially insecure password. They need direct access to RWDCs to retrieve and roll their credential. | | |
| 4 | TBD | Schema Mods and Attribute Stamping | TBD - will be filled in once applications are identified | | |
| 5 | | | | | |

| FSMO Roles | | | |
|-------------------------|-----------|--------|--|
| Role | Host | Drift? | Description |
| PDCe | Core RWDC | NO | Responsible for synchronizing time in the enterprise |
| Schema Master | Core RWDC | NO | Schema Master controls updates to the directory schema |
| Domain Naming Master | Core RWDC | NO | Responsible for making forest-wide changes to the domain name space; the only DC that can add or remove a domain from the directory. |
| RID Master | Core RWDC | NO | Processes RID Pool requests and moves objects between domains |
| Infrastructure Master | Core RWDC | NO | Updates and maintains object SIDs and DNs. All DCs will host Global Catalog |

Forest OU Structure

