

Thinfinity Workspace – Verification Checklists

1. Edge Layer (Firewall, WAF, Load Balancer)

Check Item	Config Ref.	Status
Firewall allows only TCP 443 (HTTPS/WSS)	FW-001	☐
Firewall enforces TLS 1.2 / 1.3 only	FW-002	☐
Firewall disables deep inspection for WebSocket traffic	FW-003	☐
Firewall segmentation between Edge and Orchestration confirmed	FW-004	☐
Firewall egress rules limited to NTP 123 and CRL/OCSP	FW-005	☐
WAF started in Learning Mode before enforcement	WAF-001	☐
WAF enforces HTTPS/WSS with end-to-end encryption	WAF-002	☐
WAF allows WebSocket upgrade headers (Connection / Upgrade)	WAF-003	☐
WAF excludes /saml/* and /oauth2/* endpoints from CAPTCHA	WAF-004	☐
WAF rate limiting enabled per IP or user	WAF-005	☐
WAF supports TLS 1.2 and TLS 1.3 only	WAF-006	☐
WAF validates the Origin header from trusted portals	WAF-007	☐
Load balancer listener configured for HTTPS protocol	LB-001	☐
Load balancer listening on port 443	LB-002	☐
Backend configured for HTTP re-encrypted to 9443	LB-003	☐
Load balancer backend port set to 9443	LB-004	☐
Weighted Round Robin used for session distribution	LB-005	☐
Session persistence disabled (WebSocket maintains state)	LB-006	☐
Health check path set to /health/	LB-007	☐
Health check interval 5 seconds, retries = 3	LB-008	☐
TLS versions on load balancer restricted to 1.2 / 1.3	LB-009	☐

2. Orchestration & Control Layer (Gateways, Brokers, Database, Monitoring)

Check Item	Config Ref.	Status
Gateways expose ports 9443 and 443	GTW-001	☐
Brokers joined to Active Directory domain	GTW-002	☐
Outbound access from gateways controlled to required targets only	GTW-003	☐
Load balancing across multiple gateways verified	GTW-004	☐
Brokers use port 7443 for License Service	BRK-001	☐
Brokers communicate with AD over LDAPS 636	BRK-002	☐
Brokers connect to MySQL database on port 3306	BRK-003	☐
Broker AD cache configured with periodic refresh	BRK-004	☐
Broker AD cache stores hashed credentials and group mappings	BRK-005	☐
Database deployed as managed MySQL with HA	DB-001	☐
Database restricted to access from brokers only (port 3306)	DB-002	☐
Monitoring engine uses ports 4317–4318 over HTTPS	MON-001 / MON-002	☐
Monitoring dashboard collects metrics from gateways and brokers	MON-002	☐
RDS License Server reachable over ports 135 and dynamic range	RDS-001	☐
RDS License Server provides valid CALs	RDS-002	☐

3. Workload Layer (VDI, FSLogix, Agents)

Check Item	Config Ref.	Status
No public IPs assigned to VDI instances	VDI-001	☐
Thinfinity Agent connects outbound via HTTPS 443 to gateway	VDI-002	☐
RDP 3389 open only during provisioning and then closed	VDI-003	☐
Workload subnets isolated per user group or environment	VDI-004	☐

Check Item	Config Ref.	Status
FSLogix uses SMB 445 internally for profile storage	FSL-001	☐
FSLogix profile type set to 0 (VHDX)	FSL-002	☐
Dynamic VHDX expansion enabled (IsDynamic=1)	FSL-003	☐
Local profiles deleted when VHD applies	FSL-004	☐
Force logoff on session disconnect enabled	FSL-005	☐
Disk size (SizeInMBs) defined by group (Prod=10000 / Dev=15000)	FSL-006	☐
Volume type set to vhdx	FSL-007	☐
VHD location path correctly defined to storage cluster	FSL-008	☐
Logoff wait time (768 ms) applied	FSL-009	☐

4. Cross-Layer / Security Governance

Check Item	Config Ref.	Status
All certificates issued by trusted CA	SEC-001	☐
Centralized logging configured (/__elogs__/, /__health__/)	SEC-002	☐
NTP synchronization configured on port 123	SEC-003	☐
SAML or IdP federation enabled for SSO	SEC-004	☐
Database and profile backups performed regularly	SEC-005	☐
AD authentication enforced across all access points	SEC-006	☐
Zero Trust segmentation prevents lateral movement between layers	SEC-007	☐