

CUPS 1.0(1) Deployment Guidelines for: Configuration, Capacity, Serviceability, High Availability and Security

Configuration and Admin

- The installation, upgrade, and configuration of CUPS is very similar to CUCM.
- CUPS builds off the CUCM database, extends the existing schema and contains same users and devices.
- Records are synced or copied over from the CUCM DB to the CUPS DB after installation. The initial sync operation can take a number of hours; it is dependent on the database size and system load. (e.g. 7845 2500 users: 1 hour, 7845 30000 users: 12.5 hours)
- After the initial sync is complete, any newly added users, devices and related entrees are synced to CUPS in real-time
- If the sync agent connection to CUCM is broken, it must be manually restarted in order to pick up new database entrees.
- All users, devices, numplans, are administered on CUCM. Syncing Device and capability license management also occurs on the CUCM system.

CUPS Capacity and Platforms

- CUPS 1.0(1) requires CUCM 5.0.4
- Supports newer MCS7825, MCS7835, or MCS7845 hardware platforms only. Should be maxed out with memory and hard disk.
- CUPS installations support either single or dual node configuration.
- Release 1.0(1) supports up to 1000 users on all platforms and cluster configs, single or dual node. Next release will increase these numbers. i.e. in 1.0(2), 7845 should support 2500 single node, and 5000 dual node.

CUPS Serviceability

- CUPS OAM&P leverages the CUCM framework and are integrated in the Real Time Monitoring Tool (RTMT).
- CUPS also leverages CUCM serviceability infrastructure and has the same look and feel for the serviceability web page.
- Some misleading labels/titles in RTMT, which are displayed as "Cisco Call Manager" instead of CUPS.

- On serviceability web page, some menus say "Cisco Call Manager" instead of "CUPS".
- Some performance counters for ippm, proxy and presence engine (PE) are not available in the RTMT tool.
- RTMT pre-canned performance monitoring screens are not available for CUPS product.
- CUPS proxy debug flags are not configured through serviceability, but as service parms.
- Alarms cannot be monitored in Alert Central in RTMT unless they are "threshold related".
- Some troubleshooting aspects might need "root access" to the CUPS machine. This is especially required when a core file needs to be debugged on the target machine.
- Some of the CUPS services like PE need to be re-started if debugging level needs to be changed on the fly for trouble-shooting purpose.

CUPS High Availability

- CUPS and CUCM are installed as 2 separate clusters. Requiring separate Admin and provisioning (though end user provision occurs only on CUCM)
- CUPS adopted CUCM's publisher/subscriber database technology and architecture. CUPS does not support clustering across the WAN. All nodes must on same LAN.
- Primary benefit of clustering in release 1.0(x) is to provide load sharing. Allowing processing power to be scaled past a single node's capacity.
- The CUPS/CUPC system has no automatic load balancing or failover. Neither CUPC or IPPM can detect a node failure and switchover. This must be done manually by end user.

1. When Publisher is down, some services are impacted:

- IPPM
 - Sending and receiving of new IMs are disabled.
 - IPPM settings can be viewed and modified for the current login session, but are lost once the user logs out.
- CUPC
 - All new login requests will fail
 - Users cannot update contact list.

- Admin GUI
 - The broadcast and group broadcast features will not function.
 - The IPPM Web-based logout feature will not function.
- CUCM configuration updates
 - CUCM DB change are lost until Publisher is back up and sync agent is manually restarted.

2. Subscriber Node failure:

- If subscriber node fails, only CUPC and IPPM users logged in through those nodes loose service

3. CUCM node crash or failure

- If using CUCM DNS SRV name, then subscriptions will be balanced across a set of trunks, and failure in a trunk can be routed around after subscription timeouts.
- If IP Address used, failure in that node, means that no new phone status is available.

4. CUCM Publisher DB node crash failure

- When CUCM Publisher database is down, no users or devices can be provisioned. However none of the CUPS users or services will be impacted.

Security

- Intracluster traffic is insecure. Not protected by IPSec or TLS. Recommend placing CUPS and CUCM on their own LAN.
- IPPM application is insecure. All HTTP traffic between Phone and IPPM is over TCP. IPPM login is protected by a numeric PIN which is not encrypted or hashed, but is transmitted in the clear.
- CUPC user login and configuration data is secure. Uses HTTPS, but certificates are not validated or authenticated.
- All CUPC SIP traffic to CUPS or CUCM is insecure
- UDP, TCP, TLS (mutual auth), and IPSec supported for external traffic. But IPSec is not recommended due to packet loss which occurs when the IPSec layer is dynamically negotiating new keys.
- By default no SIP endpoint can connect and send SIP traffic without being HTTP Digest challenged. ACLs can be configured to allow unrestricted traffic.
- Only users who have been assigned a CUPS license can be watched.