

## # Slurm Cluster Authentication and Authorization Using LDAP

## 1. Overview In a multi-user Slurm cluster, you typically centralize identity and access management so that compute nodes don't maintain separate /etc/passwd or /etc/group files. LDAP provides a directory service that stores user, group, and policy information centrally. Integrating LDAP ensures consistent authentication and authorization across all nodes (login, compute, and controller).

### ## 2. Authentication

### a. Components - LDAP server: Provides centralized user and group information. - PAM (Pluggable Authentication Modules): Handles authentication for login and Slurm daemons. - SSSD or nslcd: Daemon on each node that communicates with the LDAP server to fetch identity data.

### b. Flow 1. A user logs in to a Slurm login node (e.g., via SSH or srun). 2. The system uses PAM to check credentials (username/password or Kerberos ticket) against the LDAP directory. 3. SSSD/nslcd fetches user and group info from LDAP and populates it into the system's NSS (Name Service Switch) layer. 4. Once authenticated, Slurm uses the UID/GID from LDAP to authorize and track the job.

### ## 3. Authorization in Slurm

### a. Slurm's Role Slurm itself doesn't directly handle LDAP credentials. It relies on the system's account data (NSS) for user and group identity, and optionally integrates with LDAP-backed Slurm accounting databases.

### b. Authorization Flow 1. Slurm reads the user identity (UID/GID) from the system. 2. Access control decisions are based on: - Cluster configuration (AllowGroups, AllowAccounts, PrivateData, etc.) - SlurmDBD (if using accounting) - LDAP group membership (via system NSS)

### c. Common Authorization Options - Limit which users or groups can submit jobs:  
AllowGroups=cluster\_users,hpc\_team - Restrict node access by partition: PartitionName=compute  
Nodes=node[1-50] AllowGroups=research

### ## 4. Configuration Steps

### a. Install LDAP/SSSD on all nodes sudo apt install sssd libnss-sss libpam-sss

### b. Configure /etc/sssd/sssd.conf [sssd] services = nss, pam config\_file\_version = 2 domains = LDAP

```
[domain/LDAP] id_provider = ldap auth_provider = ldap ldap_uri = ldap://ldap.example.com
ldap_search_base = dc=example,dc=com ldap_tls_reqcert = allow cache_credentials = True
```

Then enable and start: sudo systemctl enable sssd sudo systemctl start sssd

### c. Update NSS and PAM /etc/nsswitch.conf: passwd: files sss group: files sss shadow: files sss  
/etc/pam.d/sshd or /etc/pam.d/slurm: auth sufficient pam\_sss.so account sufficient pam\_sss.so

### d. Configure Slurm for LDAP-backed users Ensure consistent UID/GID mapping: id username

## 5. Optional: Integrate Accounting with LDAP If project or account data are stored in LDAP, sync them with SlurmDBD via scripts using sacctmgr.

## 6. Security Best Practices - Use LDAPS or StartTLS for secure LDAP traffic. - Restrict LDAP bind credentials. - Enable caching via SSSD for performance and offline support. - Periodically sync LDAP and Slurm accounts.

