Failure Response Templates

LDAP Replication: Failure of LDAP replication will manifest itself as intermittent failures of authentication at the IdP or intermittent to persistent failures of attribute release by the IdP due to the varying connection pooling configuration of the IdP. LDAP replication failure will not affect any other component directly, e.g. the CPR and its subcomponents will continue to work.

Remediation efforts begin with identifying why LDAP replication is failing by consulting the 389 logs and addressing any underlying issues. With reasonable logging settings, 389 may not reliably report to the outside world that replication is failing. Specifically, cn=monitor may report that replication is still enabled and the replication agreements are still in place. Active investigation is necessary beginning with the 389 logs.

SQL Replication:

IdP Failures: Most outright IdP outages will be detected by AWS ELB and failing nodes will fall out of the cluster within minutes as they fail to respond at HTTPS:8443/idp/profile/Status. Nodes failing out of the pool will increase the load on other nodes and, depending on the outage mechanism, may result in exponentially increasing failure due to increasing load until every node is down, so swiftly addressing the failing nodes and/or bringing up additional nodes is important.

Users will be lightly affected by failure of a given IdP node. Only a small number of users who are in the middle of the login process will see errors, while others may lose their SSO session, requiring them to login again. For all users, subsequent login attempts starting at the SP and triggered by mechanisms such as the back button will work.

ELB is capable of firing off warnings when certain thresholds are breached or events occur and can be configured to notify administrators in the event of outright IdP node failure.

More subtle IdP issues such as failing attribute retrieval or metadata issues will not result in nodes failing out of the pool. These issues may be detected by aggressive monitoring e.g. with scripts that are capable of performing full federated login transactions, or triggered by an influx of help desk requests. Furthermore, issues of this type are more likely to impact all IdP nodes simultaneously, which will have a consequently significantly greater user impact.

Careful change management through explicit testing of any configuration modifications and anticipation of potential issues occurring independently of active configuration changes(e.g. monitoring metadata or certificate expiration dates) are paramount to preventing IdP failures.

Federated Identity Failures: