Identity & Access Management **(IAM)**

in

GitHub Enterprise

Intro

Me

@MTODD

Web Engineer

@GITHUB

LDAP, Task Lists, et al

IAM

Identity & Access Management

IAM

Identity & Access Management

- Identity & Authentication
- Access & Authorization
- Management & Automation

Problems

Customer-facing & Internal

Problems

Customer-facing & Internal

- Authentication timeouts
- Poor nested membership support
- Lacking automation
  - Deprovisioning
  - Promotion
  - Role-based access control

Problems

Customer-facing & Internal

- Product design
- Integration
- Performance
- Quality control

Solutions

Product Design & Engineering

Solutions

Product Design

Solutions

Product Design

- Automated user management
  - provisioning, deprovisioning
- Automated access control
  - Role-based access control

LDAP Sync

Product Design

USER SYNC

- Auto-suspension
- Auto-promotion
- Email, SSH public key syncing

TEAM SYNC

- Map Team to LDAP Group
- Manage Team membership via mapped LDAP Group membership

Solutions
Engineering

Solutions

Engineering

- Visibility
- Performance tuning
- Testing & QA

Refactoring

Visibility, Instrumentation, and Adaptation

Refactoring

Visibility

Net::LDAP

Solutions

Product Design & Engineering

- Maintenance & Ownership of client lib
- Protocol & Spec correctness, testing
- Reference implementations: Perl, Java, OpenLDAP, ApacheDS

Refactoring

Instrumentation

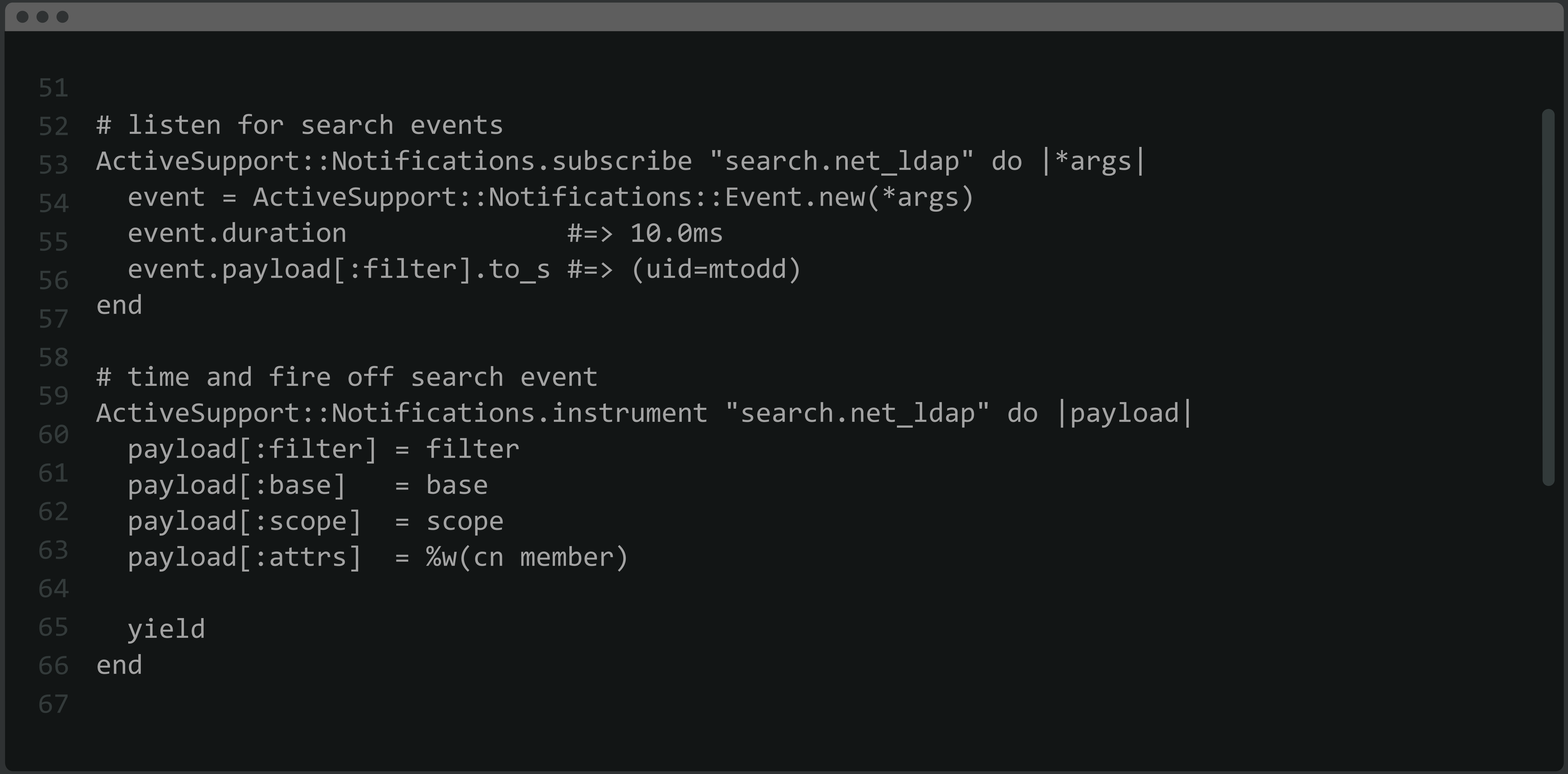
ActiveSupport::Notifications

Instrumentation

- Network reads/writes, connections
- LDAP protocol data units (PDUs)
- LDAP operations (bind, search, add, etc)

ActiveSupport::Notifications

Instrumentation



```ruby

# listen for search events
ActiveSupport::Notifications.subscribe "search.net_ldap" do |*args|
  event = ActiveSupport::Notifications::Event.new(*args)
  event.duration              #=> 10.0ms
  event.payload[:filter].to_s #=> (uid=mtodd)
end

# time and fire off search event
ActiveSupport::Notifications.instrument "search.net_ldap" do |payload|
  payload[:filter] = filter
  payload[:base]   = base
  payload[:scope]  = scope
  payload[:attrs]  = %w(cn member)

  yield
end

```

Refactoring

Adaptation

GitHub::Ldap Operations

Adaptation

- Authentication (bind)
- Membership Validation
- Member Search

GitHub::Ldap Operations

Adaptation

- Authentication (bind)
- **Membership Validation**
- Member Search

Performance Tuning

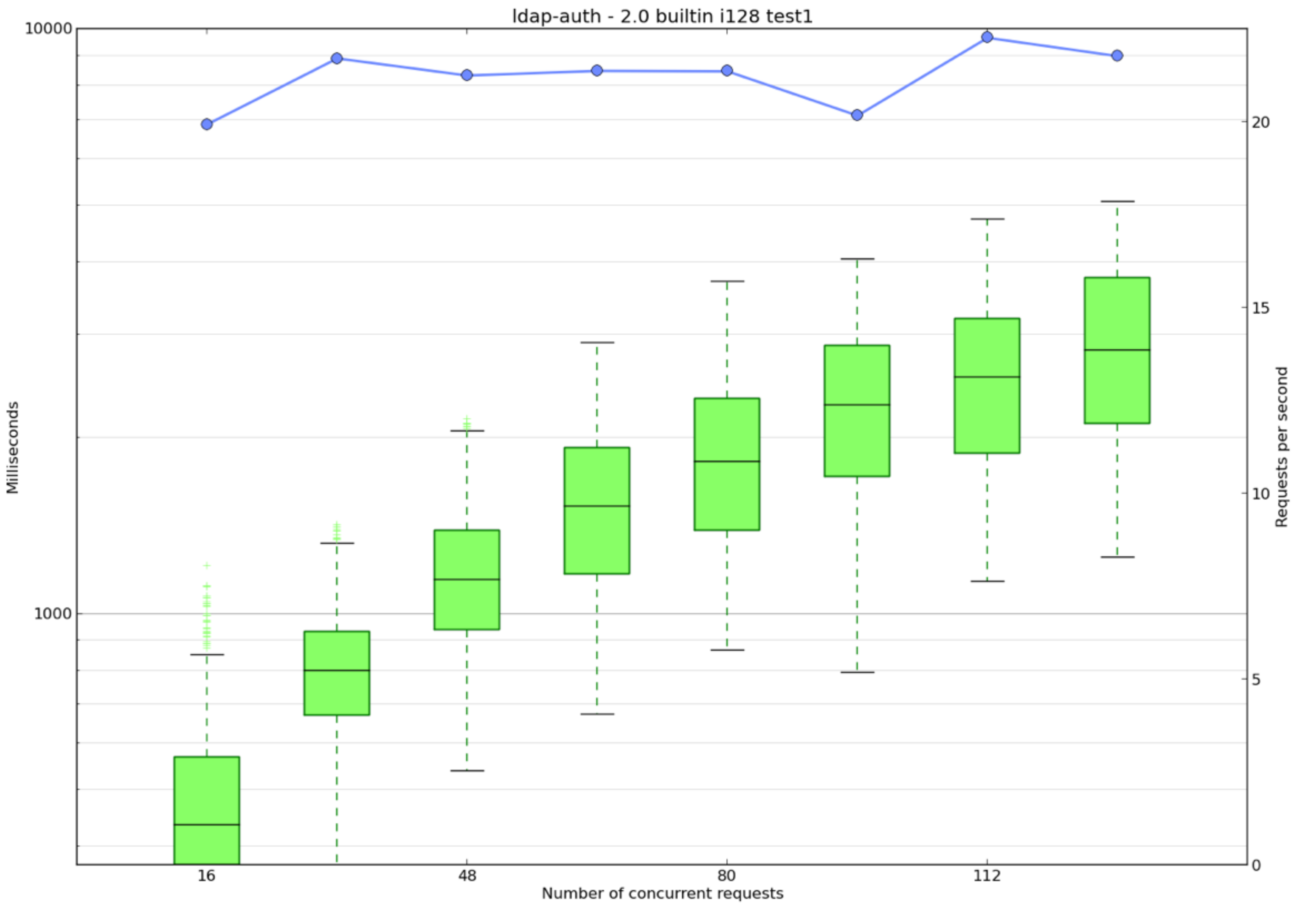
Benchmarking & Optimization

Performance Tuning

Benchmarking

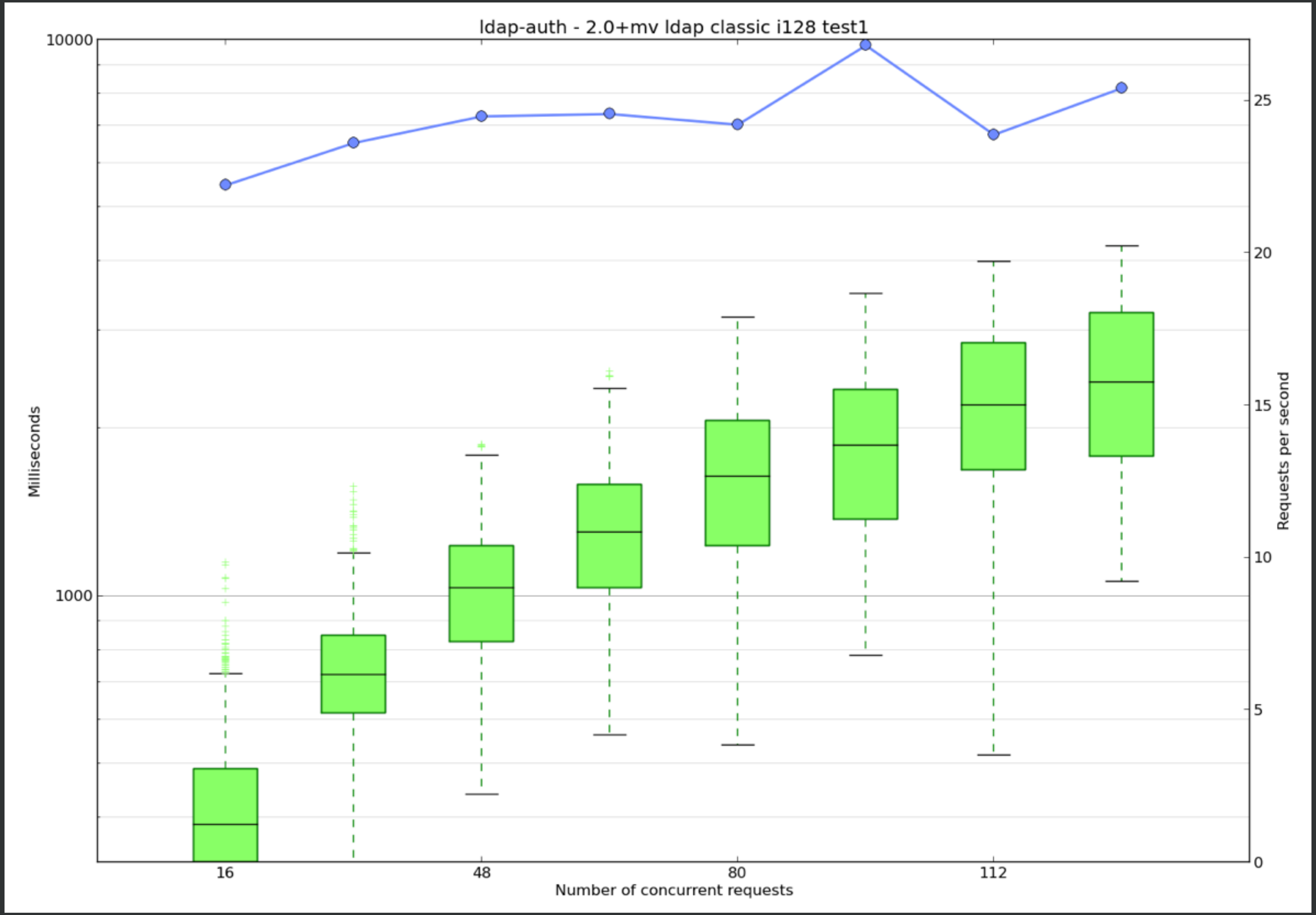
Baseline

Built-in Authentication



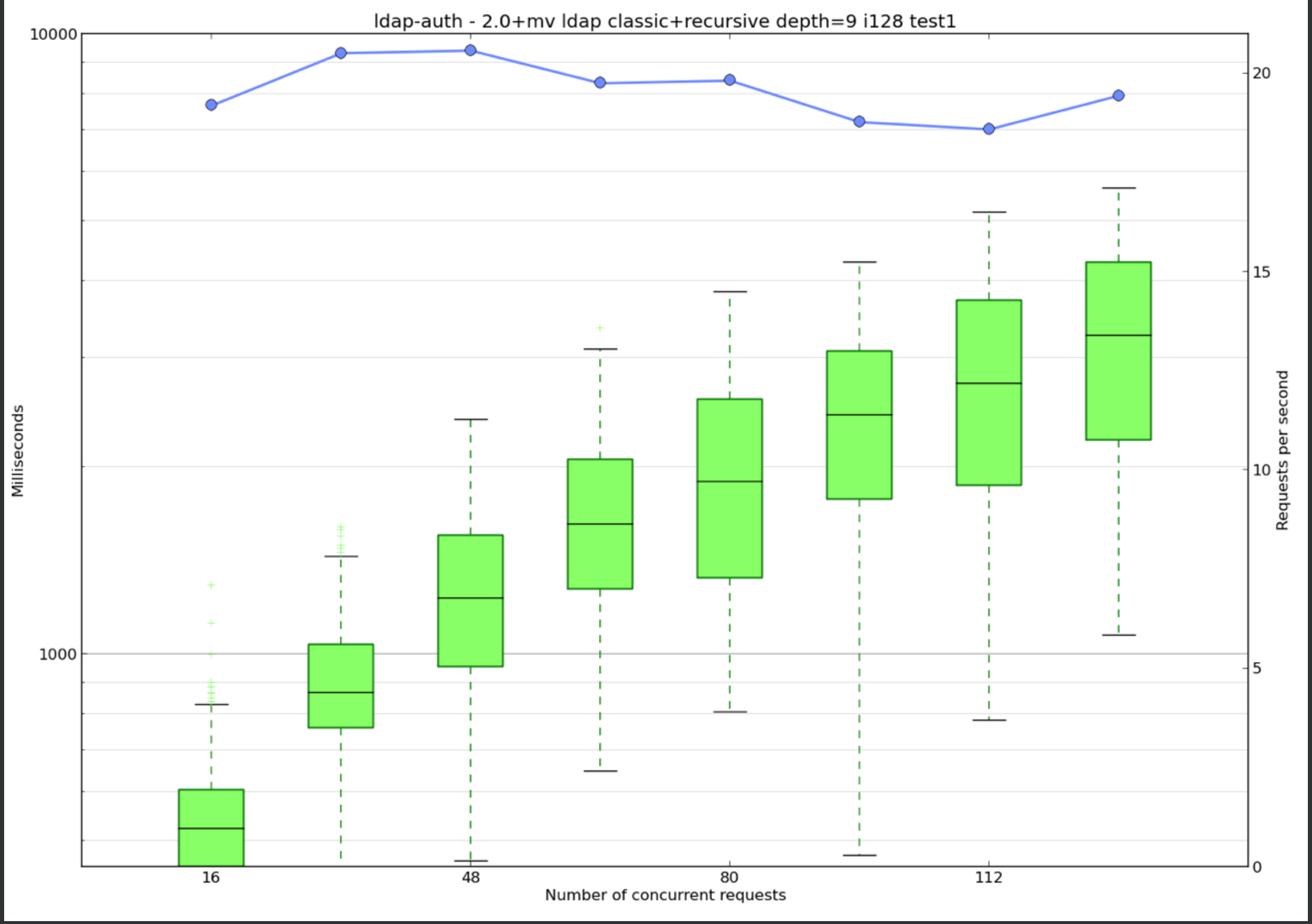
Experiment: Classic

LDAP Authentication: Best Case™ on OpenLDAP



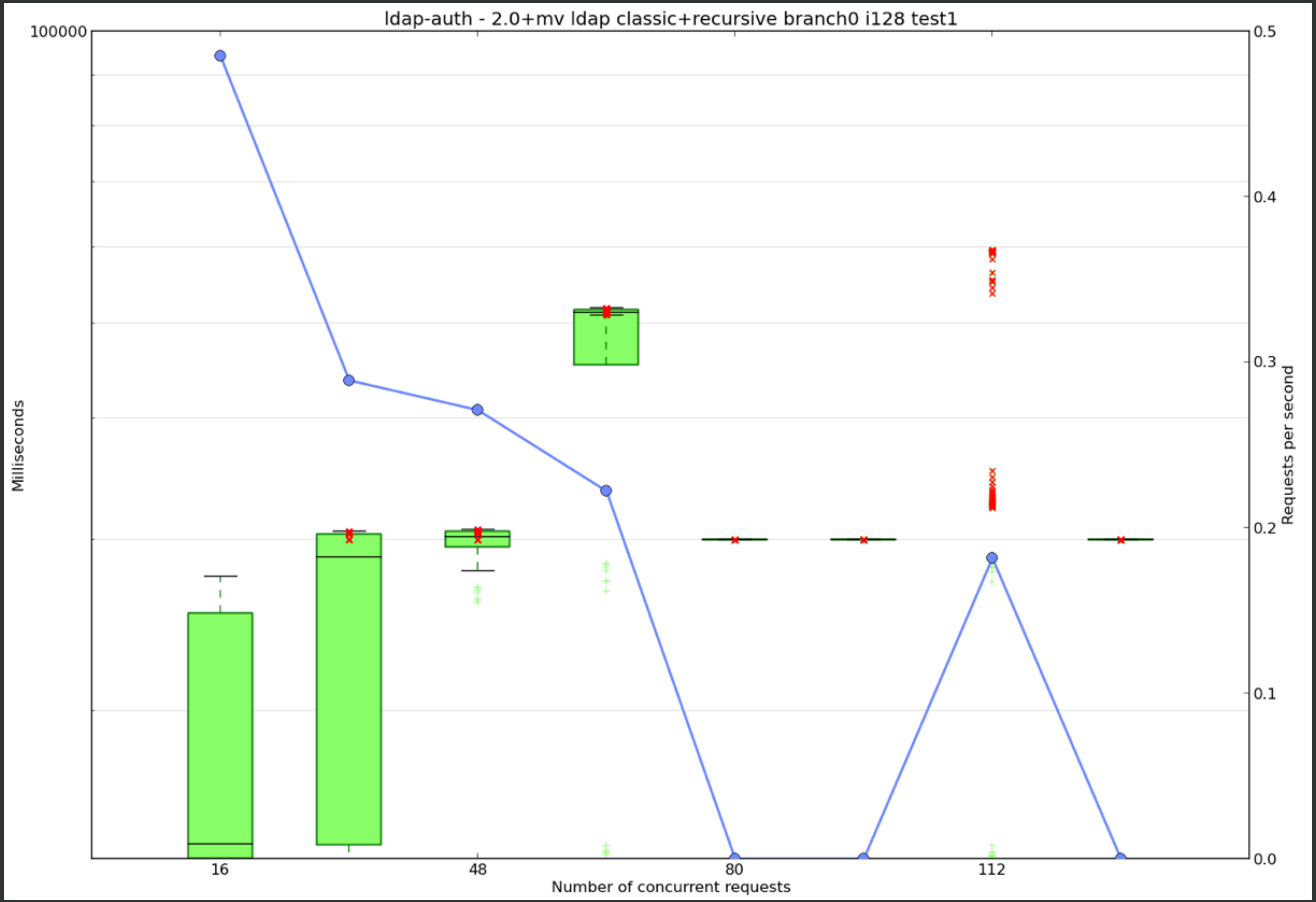
Experiment: Classic with nesting

LDAP Authentication: Best Case™ on OpenLDAP



Experiment: Classic with nesting

LDAP Authentication: Worst Case™ on OpenLDAP



Performance Tuning

Optimization

GitHub::Ldap::MembershipValidation

Optimization

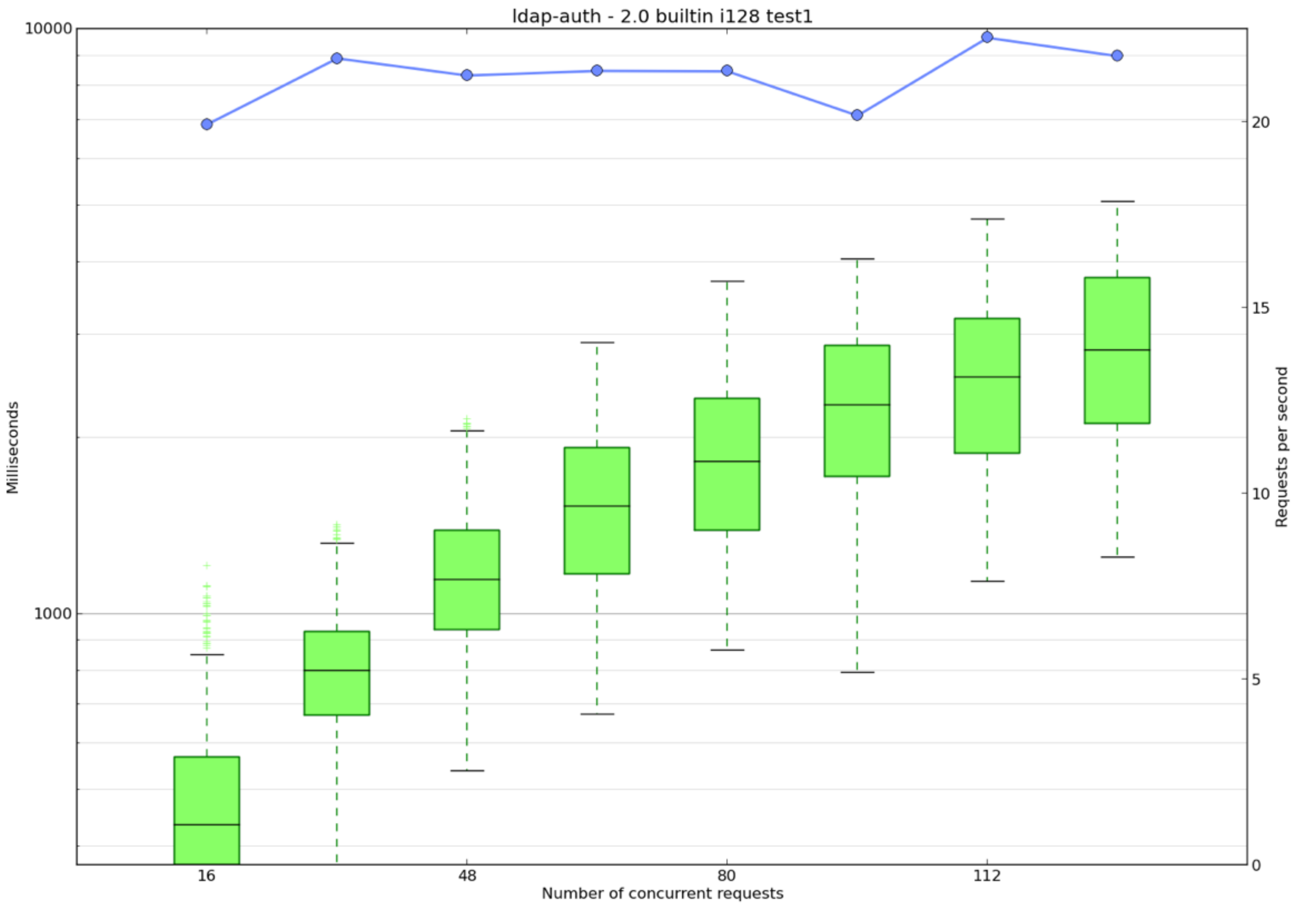
- **Classic** O(N*M)
- **Recursive** O(N)
- **Active Directory** O(1)

Performance Tuning

Benchmarking (reprise)

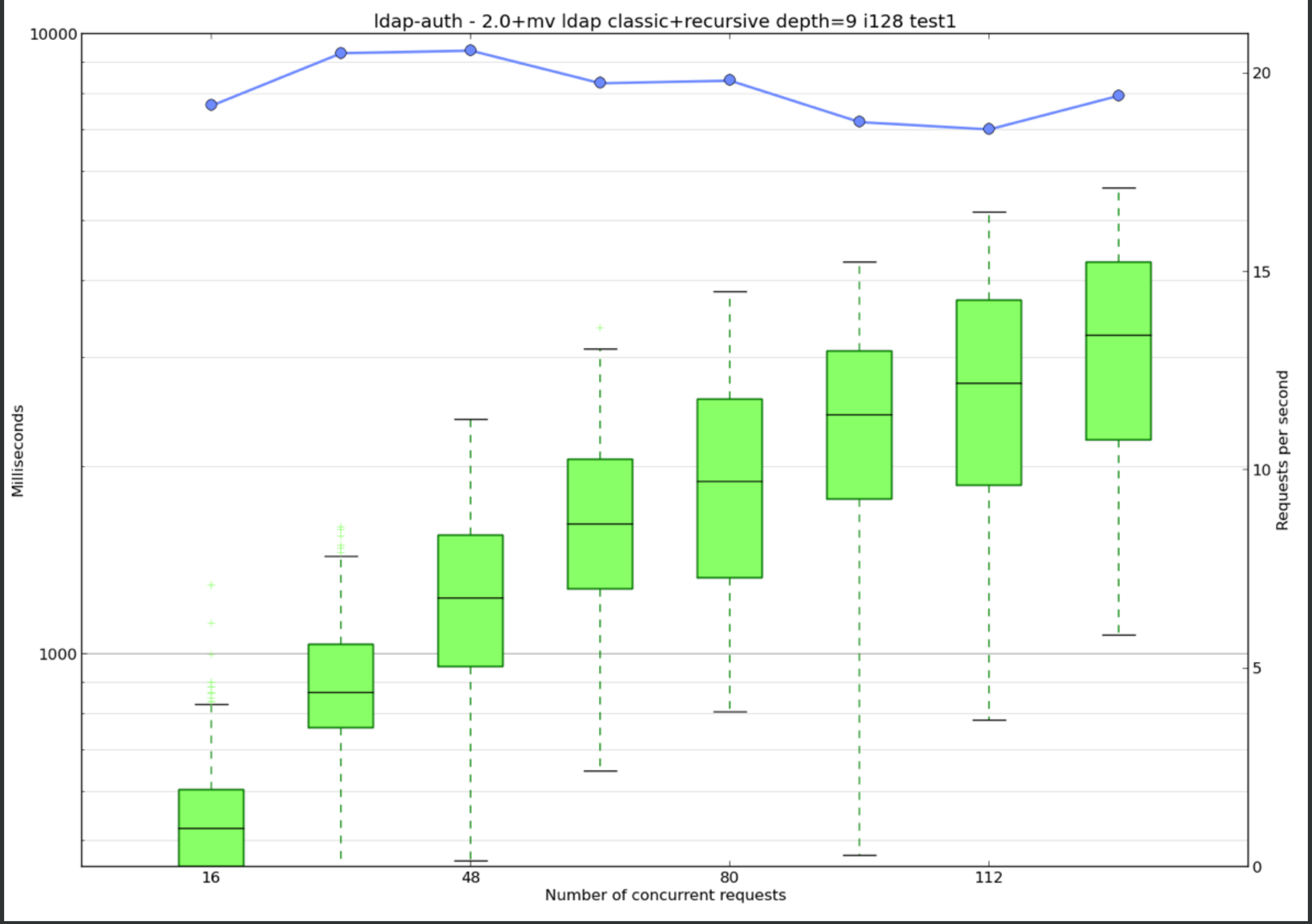
Baseline

Built-in Authentication



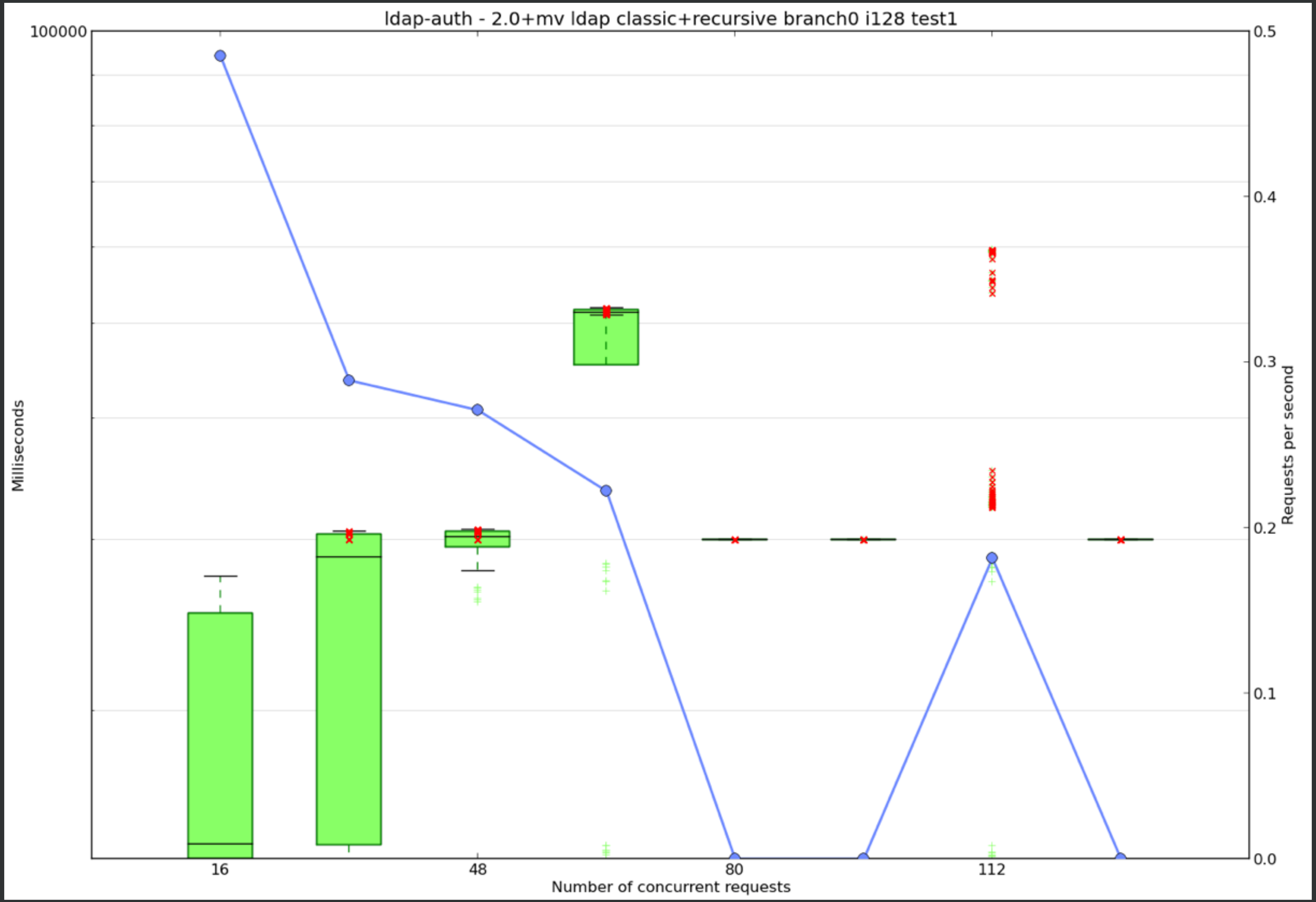
Experiment: Classic with nesting

LDAP Authentication: Best Case™ on OpenLDAP



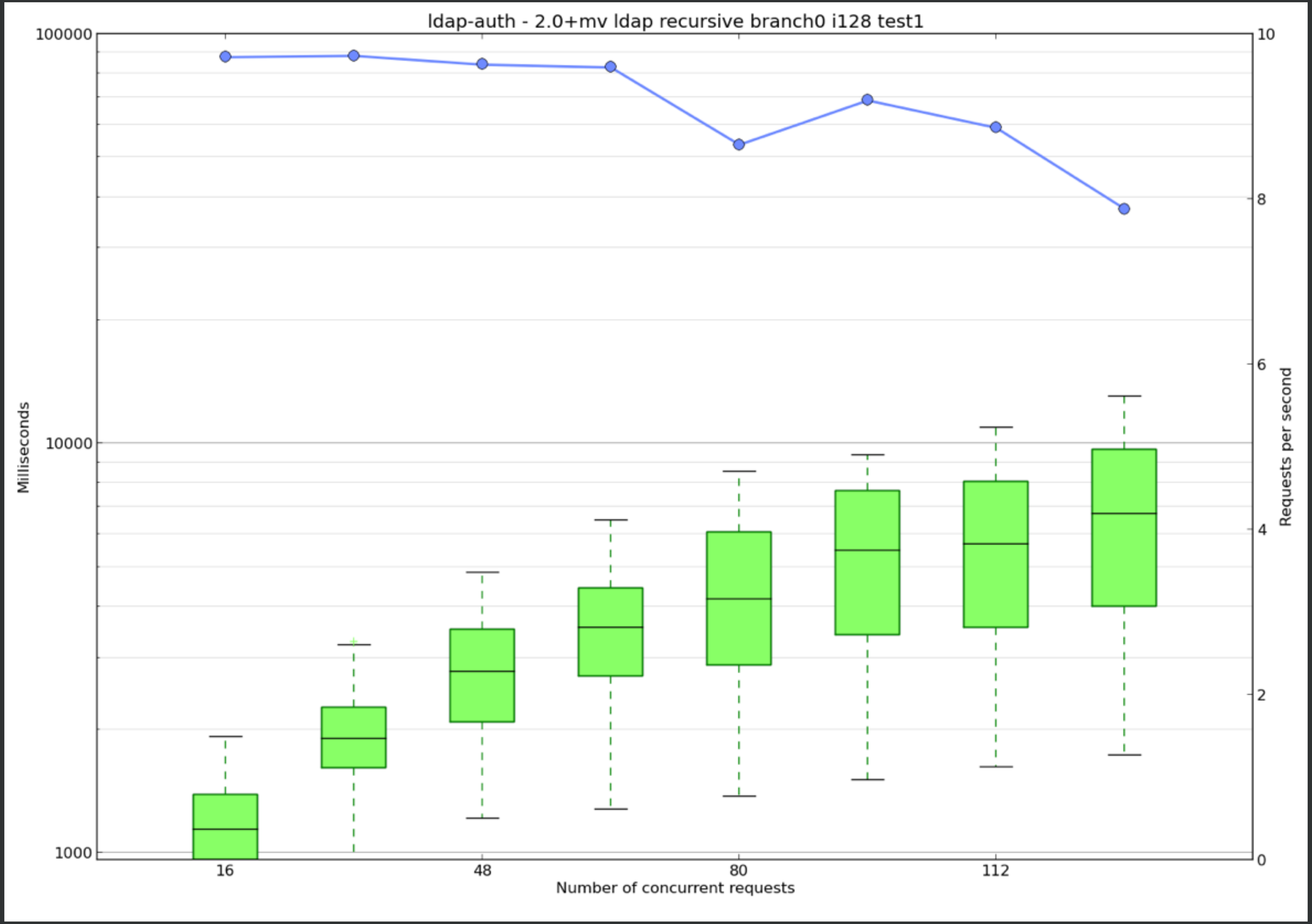
Experiment: Classic

LDAP Authentication: Worst Case™ on OpenLDAP



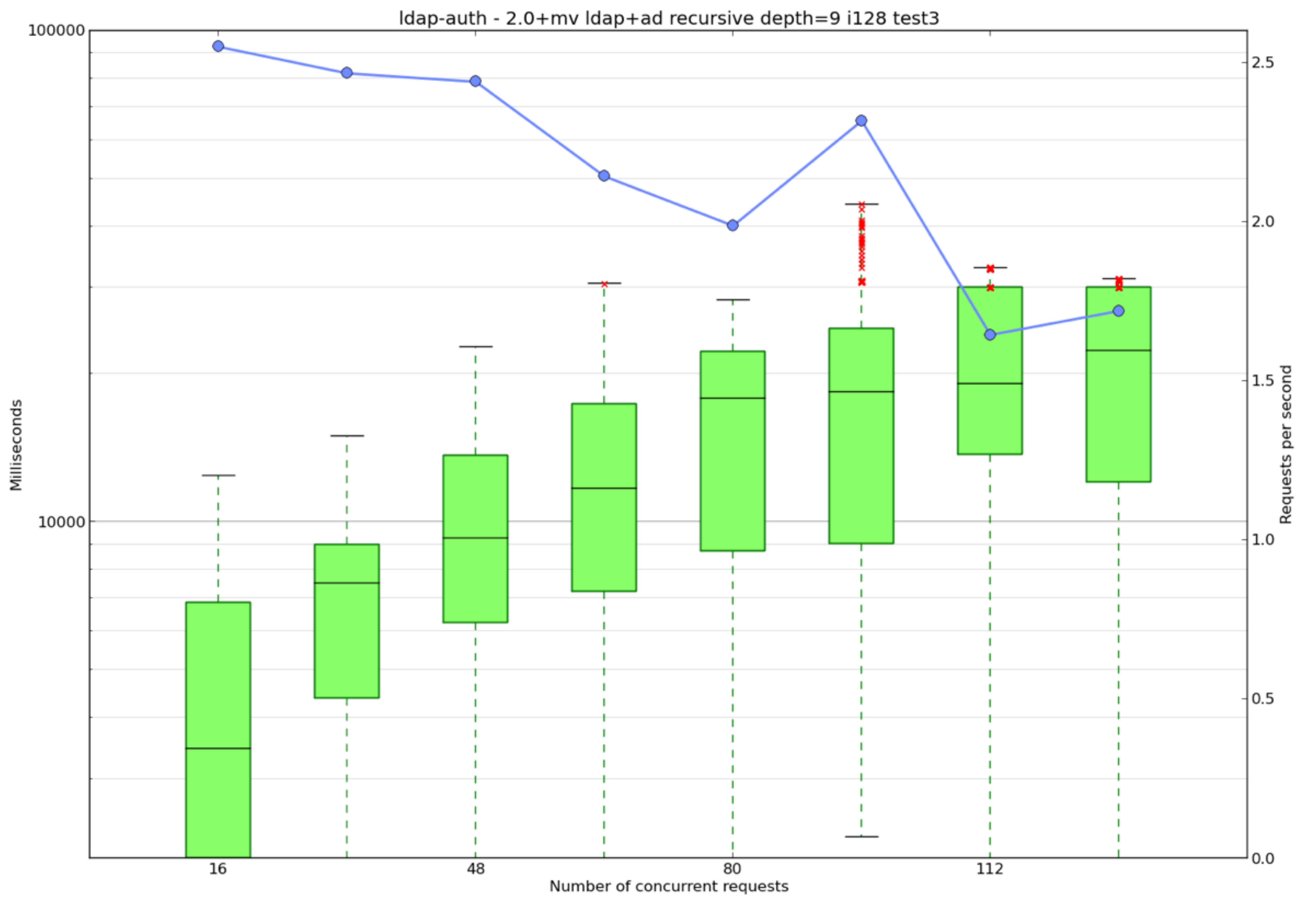
Experiment: Recursive

LDAP Authentication: Worst Case™ on OpenLDAP



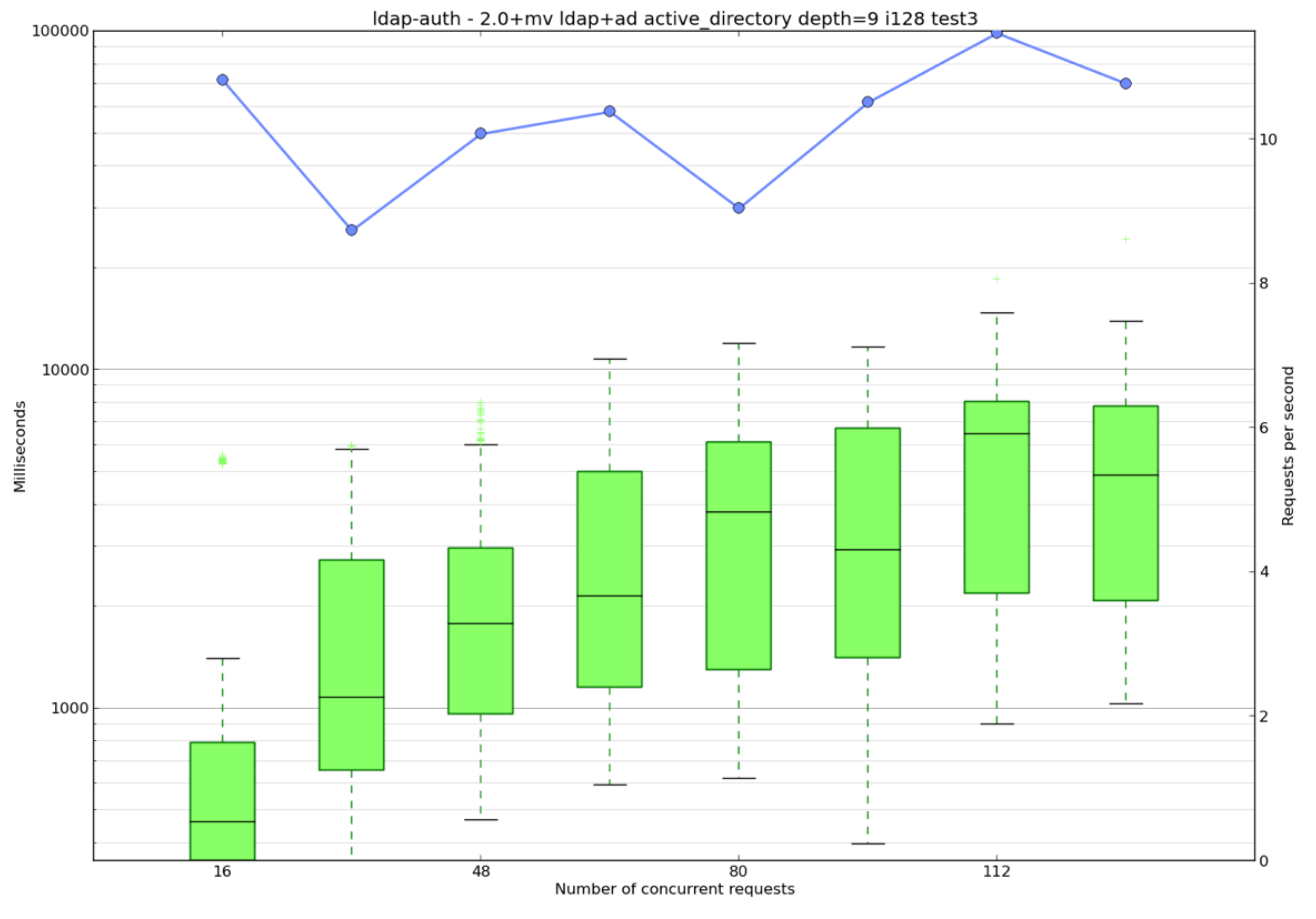
Experiment: Recursive

LDAP Authentication: Worst Case™ on Active Directory



Experiment: Active Directory "in chain"

LDAP Authentication: Worst Case™ on Active Directory



Testing

Quality Assurance & Testing Infrastructure