

Preparing for a GlideinWMS Install

1 Introduction

This document outlines the information that an administrator needs to collect prior to installing the glideinWMS. Also included are descriptions of two test installations and the assumptions, decisions, and information that went into them. Since the glideinWMS is based on Condor, an understanding of Condor will be helpful going forward. (If you don't have it now, you will by the time you are done with the glideinWMS.)

2 Basic Understanding of the glideinWMS

In order for this document (or any document about the glideinWMS for that matter) to make sense, one must have a basic understanding of what the glideinWMS actually is. The glideinWMS is a Workload Management System built on top of Condor. It uses Condor's glide-in technology to shield users from implementation details on the computing grid. It handles site selection and all the details that users generally don't want to care about. But beyond that, what IS the glideinWMS really?

Illustration 1 shows an example of the minimal install described in the Install Documentation. (<http://www.uscms.org/SoftwareComputing/Grid/WMS/glideinWMS/doc/install/>) The only minor change is that there is no GCB server in this install. In essence, the glideinWMS is a series of daemons that coordinate two condor pools. One pool is devoted to managing user jobs, the other is devoted to managing resources that will ultimately run the user jobs. To accomplish this task, the glideinWMS has several components. In Illustration 1, CMS-XEN6 has the WMS Collector and the collocated Factory installed on it. CMS-XEN7 has the VO Frontend, and CMS-XEN8 has the Pool Collector along with the user submission components.

The WMS Collector and Factory are responsible for launching glide-in pilot jobs. These are submitted to the grid sites that will run the user jobs. They can be referred to as glide-ins or pilots. They are Condor STARTD daemons that are configured to join the WMS pool. These pilot jobs are submitted to the grid sites, join the WMS pool and accept user jobs.

The Pool Collector is responsible for tracking jobs that the user submits. In Illustration 1, the pool collector and the submission components are on the same machine. A user will submit a job to the user pool (the job's information will ultimately end up in the pool collector). The User job will then be sent to one of the glide-in pilot jobs sitting on a grid site somewhere.

The VO Frontend is the glue that binds the two pools together. It monitors what glide-in pilots are available and what user jobs are submitted and matches the two together.

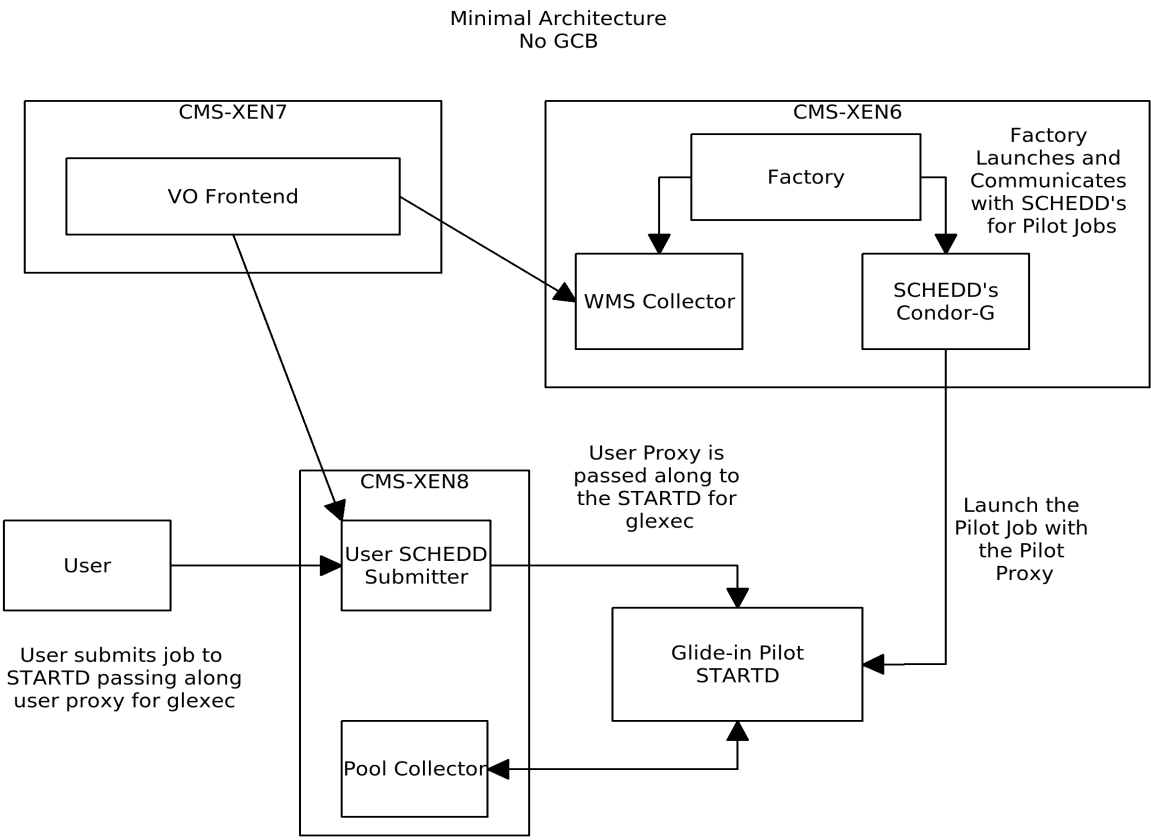
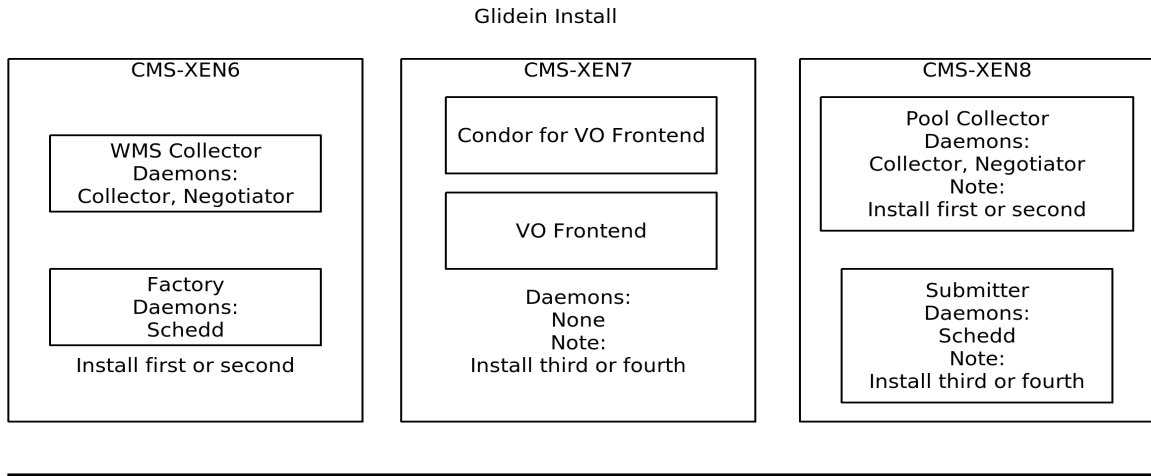


Illustration 1: Minimal Installation Described in Install Documentation

Hopefully, this short description helps to make things a little clearer. It is important to understand which daemons are talking to which other daemons. The install scripts will ask for the dn's of the certificates and/or proxies that will be used for inter process communication authentication.

3 Required Software Checklist

Before you begin make sure that the following software is either installed or that you have the software available for installation.

| Software Products | Version | Comments |
|--------------------------|--|---|
| glideinWMS | V1.6 | |
| Condor | V7.2.x (Latest version from v7.2 series) | SL3 x86 binaries should work everywhere. For x86_64 OS, you need to install 32 bit compatibility libraries. It is HIGHLY recommended that the SL3 x86 binaries be used. |
| OSG Client | Current version | |
| RRDTool | v1.2.18 (or later) | WMS Collector and collocated Factory use this package. |
| Python | v2.3.4 (or later) | |
| M2Crypto | v0.17 (or later) | WMS Collector and collocated Factory use this package. |
| HTTP Server | Latest version of Apache, TUX or Server of choice. | WMS Collector and collocated Factory use this package. |

3.1.1 SL4 Prerequisite Instructions

Need to put any SL4 specific instructions here...

```
Yum install glideinWMS # I WISH!!!
```

3.1.2 SL5 Prerequisite Instructions

To install RRDTool:

```
# yum install rrd-tool
```

To install M2Crypto:

```
# yum install m2crypto
```

After installing the HTTP server, especially if it is Apache (whether through the install script or via

yum), make sure that the configuration conforms to the security policies that your site.

4 Certificates/Proxies

Note that you will need to know AHEAD of time which components will use proxies and which will use certificates. The installation shown in Illustration 1 is configured so that the VO Frontend and the Factory use Proxies (only because there really is no other option) and all other services use certificates for GSI Authentication.

4.1.1 WMS Collector and collocated Factory

The WMS Collector can be configured to use either a proxy or a certificate. The installation shown in Illustration 1 uses a certificate for the WMS Collector. The Factory requires a valid grid/voms proxy.

The installer for the WMS Collector will ask for the VO Frontend DN.

The installer for the Factory will ask for the user proxy that the glide-in pilot jobs will be submitted as. Provide the full path to the proxy. The installer will ask for the DN's to the Pool Collector and the User Submitter. In Illustration 1, these two components both reside on CMS-XEN8. However, they can be located on separate machines. It is even recommended that the Pool Collector have its own machine if the glideinWMS is expected to handle thousands of jobs.

4.1.2 Pool Collector

The Pool Collector in Illustration 1 was configured to use a certificate. The installer will ask for the DN's of the Submitter, the user proxy that the glide-in pilot jobs use, and the DN of the proxy the VO Frontend was configured to use.

4.1.3 User Submitter

The User Submitter (Scheduler Node) is configured to use a certificate for the condor daemons. It will ask for the DN's to the certificate that the Pool Collector was configured to use and the DN to the user proxy that the glide-in pilot job was configured to use.

4.1.4 VO Frontend

The VO Frontend does not request any DN's. It talks to other daemons, but nothing talks to it. For some reason the installer requires a user proxy, but there is no technical reason that a certificate could not be used.