

PANDORAFMS
E N T E R P R I S E

Pandora FMS

LDAP Query Monitoring Administrator Manual



LDAP Query Monitoring Administrator Manual

© Artica Soluciones Tecnológicas 2005-2013

Index

1Changelog.....	3
2Introduction.....	4
3Requirements.....	5
4Compatibility matrix.....	6
5Clasification of generated software agent modules.....	7
6Installing.....	8
7Monitoring.....	9



1 CHANGELOG

Date	Autor	Change	Version
21/02/13	Mario	First version	v1r1

2 INTRODUCTION

This document has as main objective the description of the OpenLDAP server monitoring through Idap queries with no need of having a LDAP client installed in the Pandora server.

3 REQUIREMENTS

The requirements for this monitoring could work right are these:

- To have perl installed and also the perl modules Net::LDAP, Getopt::Std and File::Basename . We assume that the las modules would be installed by default in the Pandora server, but the one that we probably should install is the Net::LDAP.We could install it through the “cpan” with the command “install Net::LDAP”.
- Necessary permissions for executing the plugin by the Pandora server.
- To have connectivity with the LDAP server from the Pandora server and to know at least one user with reading permissions over the server information.

4 COMPATIBILITY MATRIX

The agent compatibility matrix is the following:

Systems where it has been tested	<ul style="list-style-type: none"> • Ubuntu 12.04 with OpenLDAP 2.4.28 • OpenSuse 12.2 with OpenLDAP 2.4.28
---	---

Systems where it should work	<ul style="list-style-type: none"> • The rest of LDAP servers
-------------------------------------	--

5 CLASIFICATION OF GENERATED SOFTWARE AGENT MODULES

This plugin is a server plugin and it is possible to create one module with each query that we want to do to the LDAP server, considering that this plugin returns only the number of returned entries by a “ldapsearch”. By default, the module is created as LDAP query, but it can be modified depending of the result that the query is going to give back.

6 INSTALLING

The installation of this plugin, as it is a server plugin, could be done through the register of plugins in the Server Management Section. We attach the pspz that automatically will be loaded in the Pandora server as a plugin with its correspondent plugin module.

The configuration for the plugin will be this:

Actualización de complemento

Nombre:

Comando del complemento:

Tipo de complemento:

Máx. tiempo de expiración:

Opción de dirección IP:

Opción de puerto:

Opción de usuario:

Opción de contraseña:

Descripción:

Actualizar

To create one module with this plugin, we should create a new plugin module and configure it this way:

Configuración de agentes - pandora - Módulos

Usando el componente del módulo:

Nombre:

Tipo:

Estado advertencia:

Umbral Flip-Flop:

Complemento:

IP destino:

Usuario:

Parámetros del complemento:

Desactivado: ☐

Grupo módulos:

Estado crítico:

Histórico de datos: ☒

Puerto:

Contraseña:

Opciones avanzadas

Actualizar

7 MONITORING

The plugin monitors the number of entries that we find when we do different queries in a LDAP server. Depending on the information that we want to monitor, we could do different LDAP queries.

To do this, we need to configure the plugin parameters right. These are the parameters that we can add:

-H, --host=STRING

Name or URI of the LDAP server. This parameter is added by default when the plugin is registered and will be defined in the field “Destination IP” of the module configuration. This field is completely necessary for the correct working of the plugin.

-p, --port=INTEGER

LDAP port. It is predefined by default as the port 389. In case it would be different to this it should be defined in the plugin parameters.

-u, --binddn=STRING

Name of the LDAP user that we should show as long as the anonymous bind would not be enabled in the LDAP server. This parameter is added by default when we register the plugin and it will be defined in the field “User” of the module configuration.

-P, --bindpw=STRING

Password of the LDAP user that we should show as long as the anonymous bind would be not enabled in the LDAP server. This parameter is added by default when the plugin is registered and will be defined in the “Password” field of the module configuration.

-Q, --filter=STRING

The plugin most important parameter. It will give to us the true value of the module. In this parameter we should put the LDAP query. Ie (objectClass=*)

-b, --base=STRING

Other parameter that is essential for the plugin working. We show in it the tree base in which we want to do the search of the query. Ie (dc=ejemplo,dc=com)

--scope=STRING

SCOPE is the starting point of a LDAP search and the depth of the base DN in order that the search should occur. There are three different options that could be assigned to the parameter:

BASE.- This value is used to show looking for the entry only in the base DN.

ONE.- This value is used to show the search of all the entries of a level under the base DN but without including the base DN and it doesn't include any entry under this level one under the base DN.

SUB.- This value is used to show the search of all the entries in all the low levels and it includes the base DN specified. It is the value predefined in the plugin and if it is none is specified in the module parametrization, will be the one that will be used.

This plugin is mainly aimed to work as server plugin but it could work in one agent that fulfills the requirement that are previously mentioned. The way to use this plugin would be creating a local module with configuration of the `módulo_exec` similar to this one:

```
module_exec perl plugin_LDAP_query_v1r1.pl -H (ip) -u (usuario) -P (pass) -Q (query) -b (base)
```