Novell
Open Enterprise Server

OPENWBEM SERVICES
ADMINISTRATION GUIDE FOR OES

Novell®

Novell Trademarks

NetWare is a registered trademark of Novell, Inc., in the United States and other countries.

Novell is a registered trademark of Novell, Inc., in the United States and other countries.

SUSE is a registered trademark of Novell, Inc., in the United States and other countries.

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide gives an overview of OpenWBEM services and Common Information Model (CIM) technologies included with Open Enterprise Server (OES) and how they relate. It also describes how to implement these services in your network and configure the OpenWBEM Common Information Model Object Manager (CIMOM) on an Open Enterprise Server running SUSE® LINUX or NetWare®.

This guide is divided into the following sections:

Audience

This guide is intended for network administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *OpenWBEM Services Administration Guide for OES*, see the Open Enterprise Server online documentation (http://www.novell.com/documentation/oes/cimom/data/front.html#bktitle).

Additional Documentation

For more in-depth information about the Distributed Management Task Force (DMTF) and its standards, see the DTMF Web site (http://www.dmtf.org/home).

For more information on the open source project OpenWBEM, see the OpenWBEM Web site (http://openwbem.org).

Documentation Conventions

In Novell® documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Overview

1

Novell® Open Enterprise Server (OES) has embraced the open standard strategies of Web-Based Enterprise Management (WBEM) proposed by the Distributed Management Task Force (DTMF) (http://www.dmtf.org/home). Implementing these strategies can substantially reduce the level of complexity associated with managing disparate systems in your network.

The following information describes a few of the components proposed by the DTMF standards. Understanding what these are and how they relate to each other can help you understand what OpenWBEM is and how you most effectively use it in your network.

- Web-Based Enterprise Management (WBEM) is a set of management and Internet standard technologies developed to unify the management of enterprise computing environments. WBEM provides the ability for the industry to deliver a well integrated set of standards-based management tools leveraging the emerging Web technologies. The DMTF has developed a core set of standards that make up WBEM:

  - A data model: the Common Information Model (CIM) standard

  - An encoding specification: CIM-XML Encoding Specification

  - A transport mechanism: CIM Operations over HTTP

- The Common Information Model (CIM) is a conceptual information model for describing management that is not bound to a particular implementation. This allows for the interchange of management information between management systems and applications. This can be either agent-to-manager or manager-to-manager communications that provide for distributed system management. There are two parts to CIM: the CIM Specification and the CIM Schema.

  The CIM Specification describes the language, naming, and meta schema. The meta schema is a formal definition of the model. It defines the terms used to express the model and their usage and semantics. The elements of the meta schema are Classes, Properties, and Methods. The meta schema also supports Indications and Associations as types of Classes, and References as types of Properties.

  The CIM Schema provides the actual model descriptions. The CIM Schema supplies a set of classes with properties and associations that provide a well understood conceptual framework within which it is possible to organize the available information about the managed environment.

- The Common Information Model Object Manager (CIMOM) is a CIM object manager or, more specifically, an application that manages objects according to the CIM standard.

- CIMOM providers are software that performs specific tasks within the CIMOM that are requested by client applications. Each provider instruments one or more aspects of the CIMOM's schema.

Open Enterprise Server contains the CIMOM from the OpenWBEM project (http://openwbem.org).

Novell LIFE and OpenWBEM packages (on Linux) or the owcimomd (WBEM CIMOM Daemon module and other LIBC modules on NetWare®) include a set of basic Novell providers, including some sample providers, and a base set of accompanying Novell schemas.

As Novell moves forward with OpenWBEM and development of specific providers, it will provide tools that offer the following important features:

- Efficient monitoring of network systems
- Recording of alterations within existing management configurations
- Hardware inventory and asset management

Understanding how the OpenWBEM CIMOM is set up and how to configure it can help you monitor and manage disparate system in your network with more confidence and ease.

1.1 What's Next

For information about the tasks you might want to perform, see the following table.

Table 1-1 *Information Index*

Task	See
How OpenWBEM coexists with other platforms on your network	"Coexistence and Migration" on page 11
Setting Up OpenWBEM	"Setting Up OpenWBEM" on page 13
Configuring OpenWBEM	"Changing the OpenWBEM CIMOM Configuration" on page 19

Coexistence and Migration

<div style="text-align: right; font-size: 3em">2</div>

The section contains the following information:

2.1 Coexistence

This section provides information regarding the compatibility and coexistence of OpenWBEM Services with existing networks containing NetWare® or Linux platforms.

2.1.1 Compatibility

The following table summarizes the compatibility of OpenWBEM Services with various operating systems:

Table 2-1   Compatibility of OES Services on Various Versions of Operating Systems

Operating System	Compatible Versions
NetWare	OES on NetWare
	NetWare 6.5 SP3 or later
Linux	SUSE® LINUX OES
	SUSE LINUX Enterprise Server 9 SP1

2.1.2 Coexistence Issues

Unknown.

2.2 Migration

No issues. This service is new in Novell® Open Enterprise Server.

Setting Up OpenWBEM

<div style="text-align:right">3</div>

When you install any component of Novell® Open Enterprise Server (OES) on Linux or install or upgrade to OES on NetWare®, OpenWBEM is installed by default. If you want to run OpenWBEM on a NetWare 6.5 SP3 server, you must install the files manually.

This section includes the following information:

3.1 Starting, Stopping, or Checking Status for OWCIMOMD

When OpenWBEM is installed, it is started by default on OES on Linux and on OES on NetWare. The following table explains how to start, stop, and check status for OWCIMOND.

Table 3-1 *Commands for Managing OWCIMOMD*

Task	Linux Command	NetWare Command
Start owcimomd	As root in a console shell, enter `rcowcimomd start`.	As user Admin or equivalent at the System Console, enter `openwbem`.
Stop owcimomd	As root in a console shell, enter `rcowcimomd stop`.	As user Admin or equivalent at the System Console, enter `unload owcimomd`.
Check owcimomd status	As root in a console shell, enter `rcowcimomd status`.	As user Admin or equivalent at the System Console, enter `modules owcimomd`. You can also view the list of loaded modules using Novell Remote Manager.

3.2 Ensuring Secure Access

The default setup of OpenWBEM is relatively secure. However, you might want to review the following to ensure access to OpenWBEM components is as secure as desired for your organization.

3.2.1 Certificates

Secure Socket Layers (SSL) transports require a certificate for secure communications to occur. When OES is installed, OpenWBEM has a self-signed certificate generated for it.

If desired, you can replace the path for the default certificate with a path to a commercial certificate that you have purchased or with a different certificate that you have generated in the `http_server.SSL_cert = ` *`path_filename`* setting in the `openwbem.conf` file.

The default generated certificate is in the following locations:

Table 3-2 *Default Locations for Generated Certificates*

Platform	File Location
Linux	`/etc/openwbem/hostkey+cert.pem`
NetWare	`sys:/system/cimom/etc/openwbem/hostkey+cert.pem`

If you want to generate a new certificate, use the following commands. Running these commands replaces the current certificate, so Novell recommends making a copy of the old certificate before generating a new one.

Table 3-3 *Commands for Generating Certificates*

Platform	Command
Linux	As root in a console shell, enter `sh/etc/openwbem/owgencert`.
NetWare	As user Admin or with equivalent rights in a Bash console shell, enter `/system/cimom/etc/openwbem/owgencert`. To get a bash prompt, enter `bash` at the System Console prompt. To exit the bash console shell, enter `exit`. For more information about using bash commands on NetWare, see "BASH" in the *Utilities Reference for OES*.

If you want to change the certificate that OpenWBEM uses, see "Changing the Certificate Configuration" on page 26.

3.2.2 Ports

OpenWBEM is configured by default to accept all communications through a secure port, 5989. The following table explains the port communication setup and recommended configuration.

Table 3-4 *Port Communication Setup and Rcommended Configurations*

Port	Type	Notes and Recommendations
5989	Secure	The secure port that OpenWBEM communications use via HTTPS services.
		This is the default configuration.
		With this setting, all communications between the CIMOM and client applications are encrypted when sent over the Internet between servers and workstations. Users must authenticate through the client application to view this information.
		Novell recommends that you maintain this setting in the configuration file.
		In order for the OpenWBEM CIMOM to communicate with the necessary applications, this port must be open in routers and firewalls if they are present between the client application (iManager plug-in) and the nodes being monitored.
5988	Unsecure	The unsecure port that OpenWBEM communications use via HTTP services.
		This setting is disabled by default.
		With this setting, all communications between the CIMOM and client applications are open for review when sent over the Internet between servers and workstations by anyone without any authentication.
		Novell recommends that you use this setting only when attempting to debug a problem with the CIMOM. As soon as the problem is resolved, set this back to the secure port, 5989.
		In order for the OpenWBEM CIMOM to communicate with the necessary applications, this port must be open in routers and firewalls if they are present between the client application (iManager plug-in) and the nodes being monitored.

If you want to change the default port assignments, see .

3.2.3 Authentication

The following authentication settings are set and enabled as the default for each platform for OpenWBEM in OES.

You can change any of the default settings. See .

Linux

On Linux, the following settings are default:

- `http_server.allow_local_authentication = true`
- `http_server.ssl_client_verification = disabled`
- `http_server.use_digest = false`
- `owcimomd.allow_anonymous = false`
- `owcimomd.allowed_users = *`
- `owcimomd.authentication_module = /opt/novell/lib/openwbem/`
  `authentication/libnovellauthentication.so`

On Linux, the OpenWBEM CIMOM is PAM enabled; therefore the following can occur:

- Local users can authenticate to the OpenWBEM CIMOM with local user credentials.
- If LUM is installed on the server where the OpenWBEM CIMOM is running, then the Linux/LUM-enabled user can authenticate to the OpenWBEM CIMOM.
- If a Linux/LUM-enabled user has the Supervisor right for the Entry Rights property for the UNIX Workstation object that represents the Linux server, the OpenWBEM CIMOM grants that user Root privileges to that Linux server.

NetWare

On NetWare, the following settings are default:

- `http_server.allow_local_authentication = false`
- `http_server.ssl_client_verification = disabled`
- `http_server.use_digest = false`
- `owcimomd.allow_anonymous = false`
- `owcimomd.allowed_users = *`
- `owcimomd.authentication_module = /system/cimom/lib/openwbem/`
  `authentication/libnetwareauthentication.nlm`
  `ldap_auth.ldap_host = 127.0.0.1`
  `ldap_auth.cert_file = /public/RootCert.der`

  You need to reconfigure the LDAP settings as shown in the following table. To change these settings, see .

Table 3-5 *Recommended Changes for LDAP Settings*

Setting	Recommended Change
ldap_auth.ldap_host	Change from a local IP address to the IP address or DNS name of the LDAP server for your network.
ldap_auth.cert_file	Change from the `public/RootCert.der` file on the local server to the `RootCert.der` file for the LDAP server in your network.

Setting	Recommended Change
ldap_auth.searchbase	Set the LDAP search base to a container where the set of users that are using OpenWBEM is in the tree; otherwise, the search starts at the root of the tree.

The following additional LDAP settings are recognized by owcimom.nlm:

- ldap_auth.ldap_port = 636
- ldap_auth.bind_timelimit = 3
- ldap_auth.binddn = anonymous
- ldap_auth.bindpw = N/A
- ldap_auth.search_timelimit = 10 seconds
- ldap_auth.searchscope = sub
- ldap_auth.user_cachesize = 10 entries

If you want to override these setting, you need to add them to the openwbem.conf file and make the changes as desired. To change these settings, see "Configuring Additional LDAP Settings for NetWare" on page 24.

3.3 Setting Up Logging

By default, logging for OpenWBEM is set up as follows.

You can change any of the default settings. For more information, see "Changing the Default Logging Configuration" on page 27.

3.3.1 Linux

On Linux, the following settings are default:

- log.main.components = *
- log.main.level = ERROR
- log.main.type = syslog

This means that owcimomd logging is set up to go to the /var/log/messages file or to other files depending on the configuration of syslogd. It logs all errors for all components (owcimomd).

3.3.2 NetWare

On NetWare, the following settings are default:

- log.main.components = *
- log.main.level = ERROR
- log.main.location = /system/cimom/var/owcimomd.log
- log.main.max_backup_index = 1
- log.main.max_file_size = 1000
- log.main.type = file

This means that owcimomd logging is set up to go to the
`sys:\system\cimom\var\owcimond.log` file. The default file size is 1000 KB with one
backup file. It logs all errors for all components (owcimomd).

3.4 Installing OpenWBEM on a Server Running NetWare 6.5 SP3 or Later

When you upgrade a server from NetWare 6.5 SP2 to NetWare 6.5 SP3 or later, OpenWBEM is not
installed by default. However, the `cimom.zip` file for installing OpenWBEM is available for
manually installing OpenWBEM to a server that you have upgraded to NetWare 6.5 SP3 or later.
You can find this file on the *NetWare 6.5 SP3 Products CD* in the `products/openwbem`
directory.

1 Insert the *NetWare 6.5 Products CD* into the CD-ROM drive.

2 Unzip the `cimom.zip` file to the root of volume sys: on the server.

3 Generate a certificate for use by openwbem.

As user Admin or equivalent, enter the following command in a Bash console shell:

`/system/cimom/etc/openwbem/owgencert`

To get a bash prompt, enter `bash` at the System Console prompt.

To exit the bash console shell, enter `exit`.

For more information about using bash commands on NetWare, see "BASH" in the *Utilities
Reference for OES*.

4 As user Admin or equivalent, enter the following command at the System Console prompt,
`openwbem`.

5 (Optional) If you want to make sure owcimomd is running every time the server is restarted,
add the following command to the `autoexec.ncf` file:

`openwbem.ncf`

Changing the OpenWBEM CIMOM Configuration

4

When OpenWBEM CIMOM (owcimomd) starts, it receives all of its commands for running from the `openwbem.conf` file. The `openwbem.conf` file is located in the following locations:

Table 4-1 *Openwbem.conf File Locations*

Platform	File Location
Linux	`/etc/openwbem/openwbem.conf`
NetWare®	`sys:\system\cimom\etc\openwbem\openwbem.conf`

Any setting that has the options commented out with a semicolon (;) or pound sign (#) uses the default setting.

When making changes to this file, you can use any *text* editor that saves the file in a format that is native to the platform you are using.

You can change any of the settings in the `openwbem.conf` file. This section discusses the following configuration settings:

4.1 Changing the Authentication Configuration

When changing the Authentication configuration, there are several things that you can control:

- Who can access the CIMOM
- Which LDAP server to use (on NetWare)
- Where the LDAP search for users begins (on NetWare)
- What authentication module is used

See the following settings:

4.1.1 http_server.allow_local_authentication

Purpose

Directs the http_server to allow local authentication without supplying a password, relying on local system file permissions.

You can use this setting with the Basic or Digest settings.

Syntax

`http_server.allow_local_authentication = `*`option`*

Option	Use
false	Disable local authentication.
	This is the default setting for NetWare.
true	Enables local authentication.
	This is the default setting for Linux.

Example

`http_server.allow_local_authentication = false`

4.1.2 http_server.digest_password_file

Purpose

Specifies a location for the password file. This is required if the http_server.use_digest setting is enabled.

Syntax

`http_server.digest_password_file = `*`path_filename`*

The following are the default paths and filenames for the digest password files:

Platform	File Location
Linux	/etc/openwbem/digest_auth.passwd

Platform	File Location
NetWare	`/system/cimom/etc/openwbem/digest_auth.passwd`

Example

```
http_server.digest_password_file = /etc/openwbem/
digest_auth.passwd
```

4.1.3 http_server.ssl_client_verification

Purpose

Determines whether the server should attempt to authenticate clients with SSL Client Certificate verification.

This setting is disabled by default.

Syntax

```
http_server.ssl_client_verification = option
```

Option	Use
autoupdate	Specifies the same functionality as the Optional option; however, previously unknown client certificates that pass HTTP authentication are added to a trust store so that subsequent client connections with the same certificate do not require HTTP authentication.
disabled	Disables client certificate checking. This is the default setting.
optional	Allows a trusted certificate to be authenticated (no HTTP authentication is necessary). Also allows an untrusted certificate to pass the SSL handshake if the client passes the HTTP authentication.
required	Requires a trusted certificate for the SSL handshake to succeed.

Example

```
http_server.ssl_client_verification = disabled
```

4.1.4 http_server.ssl_trust_store

Purpose

Specifies a directory containing the OpenSSL trust store.

Syntax

```
http_server.ssl_trust_store = path
```

The following are the default paths for the trust store files.

Platform	File Location
Linux	/etc/openwbem/truststore
NetWare	/system/cimom/etc/openwbem/truststore

Example

```
http_server.ssl_trust_store = /etc/openwbem/truststore
```

4.1.5 http_server.use_digest

Purpose

Directs the HTTP server to use Digest authentication, which bypasses the Basic authentication mechanism. To use digest, you must set up the digest password file using `owdigestgenpass`.

Digest doesn't use the authentication module specified by the owcimomd.authentication_module configuration setting.

Syntax

```
http_server.use_digest = option
```

Option	Use
false	Enables the Basic authentication mechanism.
true	Disables the Basic authentication mechanism.
	This is the default setting.

Example

```
http_server.use_digest = true
```

4.1.6 owcimomd.ACL_superuser

Purpose

Specifies the username of the user that has access to all Common Information Model (CIM) data in all namespaces maintained by the owcimomd. This user can be used to administer the `/root/security` name space, which is where all ACL user rights are stored.

ACL processing is not enabled until the `OpenWBEM_Acl1.0.mof` file has been imported.

Syntax

```
owcimomd.ACL_superuser = username
```

Example

```
owcimomd.ACL_superuser = root
```

4.1.7 owcimomd.allowed_anonymous

Purpose

Enables or disables anonymous logins to owcimond.

Syntax

```
owcimomd.allowed_anonymous = option
```

Option	Use
false	Requires login with a username and password to access owcimomd data.
	This is the default and recommended setting.
true	Allows anonymous logins to owcimomd.
	This disables authentication. No username or password is required to access owcimomd data.

Example

```
owcimomd.allowed_anonymous = false
```

4.1.8 owcimomd.allowed_users

Purpose

Specifes a list of users who are allowed to access owcimomd data.

Syntax

```
owcimomd.allowed_users = option
```

Option	Use
username	Specifies one or more users who are allowed to access the owcimomd data.
	Separate each username with a space.
*	Allows all users to authenticate (for example, if you choose to control access with ACLs instead).
	This option is enforced for all authentication methods unless owcimomd.allow_anonymous is set to True.
	This is the default setting.

Example

```
owcimomd.allowed_users = bcwhitely jkcarey jlanderson
```

4.1.9 owcimomd.authentication_module

Purpose

Specifies the authentication module that is used by owcimomd. This setting should be an absolute path to the shared library containing the authentication module.

Syntax

```
owcimomd.authentication_module = path_filename
```

The following are the default paths and filenames for the authentication modules:

Platform	File Location
Linux	`/opt/novell/lib/openwbem/authentication/` `libnovellauthentication.so`

NetWare	`/system/cimom/lib/openwbem/authentication/`
	`libnetwareauthentication.nlm`
	ldap_auth.ldap_host = 127.0.0.1
	ldap_auth.cert_file = `/public/RootCert.der`
	ldap_auth.searchbase = o=novell

Example on Linux

```
owcimomd.authentication_module = /opt/novell/lib/openwbem/
authentication/libnovellauthentication.so
```

Example on NetWare

```
owcimomd.authentication_module = /system/cimom/lib/openwbem/
authentication/libnetwareauthentication.nlm
ldap_auth.ldap_host = 192.155.27.1
ldap_auth.cert_file = /public/RootCert.der
ldap_auth.searchbase = ou=users,ou=provo,o=example_company
```

Configuring Additional LDAP Settings for NetWare

The following table lists the additional LDAP settings that are recognized by owcimom.nlm and explains their configuration options:

Table 4-2 *Configuration Options for Additional LDAP Settings Recognized by OWCIMOM.NLM*

Setting with Default	Configuration Options
`ldap_auth.bind_timelimit = 3`	Specifies the time (in seconds) that owcimomd spends binding to LDAP as a given user.

Setting with Default	Configuration Options
`ldap_auth.binddn = anonymous` `ldap_auth.bindpw = N/A`	If you want to change these from an anonymous bind, you must specify a fully distinguished name to bind to the server with and a password. For example: ldap_auth.binddn cn=manager, dc=example, dc=com ldap_auth.bindpw=secret
`ldap_auth.ldap_port = 636`	If you change the secure port that LDAP is configured to, change this port number.
`ldap_auth.searchscope = sub`	Options: sub, one **sub:** Sets the LDAP search to search the container specified in the ldap_auth.searchbase setting and all its subcontainers. Example context: o=example_company ou=provo ou=provo,ou=users ou=provo,ou=sales ou=provo,ou=engineers For example, if the searchbase context were set to ou=provo,o=example_company and the searchscope were set to sub, then the Provo container and all its subcontainers would be searched. **one:** Sets the LDAP search to search only the container specified in the ldap_auth.searchbase setting. For example, if the searchbase context were set to ou=users,ou=provo,o=example_company and the searchscope were set to one, then only the Users container would be searched.
`ldap_auth.search_timelimit = 10`	Specifies the amount of time (in seconds) that owcimomd spends seaching for a user in LDAP.
`ldap_auth.user_cachesize = 10`	Specifies the number of user authentication entries that are cached. Range: 0 to 1000 entries.

4.1.10 simple_auth.password_file

Purpose

Specifies the path to the password file when the simple authentication module is used.

This setting is disabled by default.

Syntax

`simple_auth.password_file = path_filename`

Linux Example

```
simple_auth.password_file = /etc/openwbem/simple_auth.passwd
```

NetWare Example

```
simple_auth.password_file = /system/cimom/etc/openwbem/
simple_auth.passwd
```

4.2 Changing the Certificate Configuration

The http_server.SSL_cert setting specifies the location of the file that contains the host's private key and the certificate that is used by OpenSSL for HTTPS communications.

The hostkey+cert.pem file is located in the following default locations:

Table 4-3   Hostkey+cert.pem File Locations

Platform	File Location
Linux	/etc/openwbem/hostkey+cert.pem
NetWare	/system/cimom/etc/openwbem/hostkey+cert.pem

Syntax

```
http_server.SSL_cert = path_filename
```

Example

```
http_server.SSL_cert = /etc/openwbem/hostkey+cert.pem
```

4.3 Changing the Port Configuration

The http_server.http_port and server.https_port settings specify the port number that owcimomd listens on for all HTTP and HTTPS communications.

Syntax

```
http_server.http_port = option
```

or

```
http_server.https_port = option
```

Option	Use
Specific_port_number	Specify the specific port for HTTP or HTTPS communications.
	For HTTP, the default port is 5988.
	For HTTPS, the default port is 5989.

Option	Use
-1	Disables HTTP or HTTPS connections (for example, if you only want to support HTTPS connections).
0	Dynamically assigns a port number at run time.

Example

These settings disable the HTTP port and enable port 5989 for HTTPS communications:

```
http_server.http_port = -1

http_server.https_port = 5989
```

4.4 Changing the Default Logging Configuration

The following log settings in the `owcimomd.conf` file let you specify where and how much logging occurs, the type of errors logged, and the log size, filename, and format:

If you want to set up debug logging, see Section 4.5, "Configuring Debug Logging," on page 32.

If you want to set up additional logs, see Section 4.6, "Configuring Additional Logs," on page 33.

4.4.1 log.main.categories

Purpose

Specifies the categories the log outputs.

Syntax

```
log.main.categories = option
```

Option	Use
category_name	Specifies the categories to be logged using a space delimited list.
	The categories used in owcimomd are:
	• DEBUG
	• ERROR
	• FATAL
	• INFO
	For more information about these options, see "log.main.level" on page 30.
	If specified in this option, the predefined categories are not treated as levels, but as independent categories. No default is available; and if a category is not set, no categories are logged and the log.main.level setting is used.
*	All categories are logged.
	This is the default setting.

Example

```
log.main.categories = FATAL ERROR INFO
```

4.4.2 log.main.components

Purpose

Specifies the components that the log outputs.

Syntax

```
log.main.components = option
```

Option	Use
component_name	Specifies the components to be logged (such as owcimomd) using a space-delimited list.
	Providers can use their own components.
*	Specifies that all components are logged.
	This is the default setting.

Example

```
log.main.components = owcimomd nssd
```

4.4.3 log.main.format

Purpose

Specifies the format (text mixed with printf() style conversion specifiers) of the log messages.

Syntax

```
log.main.format = conversion_specifier
```

Option	Specifies
%%	%
%c	Component (such as owcimomd)
%d	Date
	Can be followed by a date format specifier enclosed between braces. For example, %d{%H:%M:%S} or %d{%d %b %Y %H:%M:%S}. If no date format specifier is given, then ISO8601 format is assumed.
	The only addition is %Q, which is the number of milliseconds.
	For more information about the date format specifiers, see the documentation for the strftime() function found in the <ctime> header.
%e	Message as XML CDATA. This includes the "<![CDATA[" and ending "]]>"
%F	Filename
%l	Filename and line number. For example, file.cpp(100)
%L	Line number
%M	Method name where the logging request was issued (only works on C++ compilers which support __PRETTY_FUNCTION__ or C99's __func__).
%m	Message
%n	Platform-dependent line separator character (\n) or characters (\r\n).
%p	Category, also known as level or priority.
%r	Number of milliseconds elapsed between the start of the application and the creation of the logging event.
%t	Thread ID
\n	New line
\t	Tab
\r	Line feed
\\	\
\x<hexDigits>	Character represented in hexadecimal

It is possible to change the minimum field width, the maximum field width, and justification. The optional format modifier is placed between the percent sign (%) and the conversion character. The first optional format modifier is the left justification flag, which is the minus (-) character. The optional minimum field width modifier follows, which is an integer that represents the minimum number of characters to output. If the data item requires fewer characters, it is padded with spaces on either the left or the right, according to the justification flag. If the data item is larger than the minimum field width, the field is expanded to accommodate the data.

The maximum field width modifier is designated by a period (.) followed by a decimal constant. If the data item is longer than the maximum field, then the extra characters are removed from the beginning of the data item (by default) or from the end (if the left justification flag was specified).

Examples

Log4j TTCC layout:

```
"%r [%t] %-5p %c - %m"
```

Similar to TTCC but with some fixed-size fields:

```
"%-6r [%15.15t] %-5p %30.30c - %m"
```

XML output conforming to log4j.dtd 1.2, which can be processed by Chainsaw (if used, this must be on one line; it is split up here for readability):

```
"<log4j:event logger="%c" timestamp="%d{%s%Q}" level="%p"
thread="%t">
<log4j:message>%e</log4j:message>
<log4j:locationInfo class="" method="" file="%F" line="%L"/></
log4j:event>"
```

The following is the default:

```
log.main.format = [%t]%m
```

4.4.4 log.main.level

Purpose

Specifies the level the log outputs. If set, the log outputs all predefined categories at and above the specified level.

Syntax

```
log.main.level = option
```

Option	Use
DEBUG	Logs all Debug, Info, Error, and Fatal error messages.
ERROR	Logs all Error and Fatal error messages.
	This is the default setting.
FATAL	Logs only Fatal error messages.

Option	Use
INFO	Logs all Info, Error, and Fatal error messages.

Example

```
log.main.level = ERROR
```

4.4.5 log.main.location

Purpose

Specifies the location of the log file owcimomd uses when the log.main.type setting option specifies that logging is sent to a file.

Syntax

```
log.main.location = path_filename
```

Example

```
log.main.location = /system/cimom/var/owcimomd.log
```

4.4.6 log.main.max_backup_index

Purpose

Specifies the amount of backup logs that are kept before the oldest is erased.

Syntax

```
log.main.backup_index = option
```

Option	Use
unsigned_integer_above_0	Specifies the number of backup logs kept. The default setting is 1 log file.
0	No backup logs are made and the log is truncated when it reaches the maximum file size.

Example

```
log.main.max_backup_index = 1
```

4.4.7 log.main.max_file_size

Purpose

Specifies the maximum size (in KB) that the owcimomd log can grow to.

Syntax

```
log.main.max_file_size = option
```

Option	Use
unsigned _integer_in_KB.	Limits the log to a certain size in KB.
0	Lets the log grow to an unlimited size.
	This is the default setting.

Example

```
log.main.max_file_size = 0
```

4.4.8 log.main.type

Purpose

Specifies the type of main log owcimomd uses.

Syntax

```
log.main.type = option
```

Option	Use
file	Sends all messages to a file that is identified in the log.main.location configuration setting.
	On NetWare, this is set using the file option and the log.main.location file is set to `sys:\system\cimom\var\owcimomd.log`.
null	Disables logging.
syslog	Sends all messages to the syslog interface.
	This is the default setting for Linux.

Example

```
log.main.type = syslog
```

4.5 Configuring Debug Logging

If owcimomd is run in debug mode, then the debug log is active with the following settings:

- `log.debug.categories = *`
- `log.debug.components = *`
- `log.debug.format = [%t] %m`
- `log.debug.level = *`
- `log.debug.type = stderr`

4.5.1 Debug Log with Color

If you want a color version of the debug log, use the following ASCII escape codes:

```
log.debug.format = \x1b[1;37;40m[\x1b[1;31;40m%-
.6t\x1b[1;37;40m]\x1b[1;32;40m %m\x1b[0;37;40m
```

If you want to use additional colors, use the following codes with the log.debug.format command:

Table 4-4 *Additional Color Codes for the log.debug.format Command*

Color	Codes
red	\x1b[1;31;40m
dark red	\x1b[0;31;40m
green	\x1b[1;32;40m
dark green	\x1b[0;32;40m
yellow	\x1b[1;33;40m
dark yellow	\x1b[0;33;40m
blue	\x1b[1;34;40m
dark blue	\x1b[0;34;40m
purple	\x1b[1;35;40m
dark purple	\x1b[0;35;40m
cyan	\x1b[1;36;40m
dark cyan	\x1b[0;36;40m
white	\x1b[1;37;40m
dark white	\x1b[0;37;40m
gray	\x1b[0;37;40m
reset color	\x1b[0;37;40m

4.6 Configuring Additional Logs

If you want to create additional logs, list the log names under this setting:

```
owcimomd.additional_logs = logname
```

Separate multiple lognames spaces.

Syntax

```
owcimomd.additional_logs = logname
```

For each log, the following settings apply:

- log.*log_name*.categories
- log.*log_name*.components
- log.*log_name*.format
- log.*log_name*.level
- log.*log_name*.location
- log.*log_name*.max_backup_index
- log.*log_name*.max_file_size

Example

```
owcimomd.additional_logs = errorlog1 errorlog2 errorlog3
```

Documentation Updates

A

To help you keep current on updates to the documentation, this section contains information on content changes that have been made in this *OpenWBEM Services Administration Guide for OES* since the initial release of Open Enterprise Server.

This document is provided on the Web in HTML and PDF; and is kept up to date with the documentation changes listed in this section. If you need to know whether a copy of the PDF documentation you are using is the most recent, check its publication date on the title page.

This documentation update information is grouped according to the date the changes were published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections in the *OpenWBEM Services Administration Guide for OES*.

The documentation was updated on the following dates:

A.1 December 23, 2005 (Open Enterprise Server SP2)

Updates were made to the following sections:

A.1.1 Entire Guide

Location	Change
Entire guide.	Page design reformatted to comply with revised Novell® documentation standards.

A.1.2 Setting Up OpenWBEM

Location	Change
In Table 3-3 on page 14 and in Step 3 in "Installing OpenWBEM on a Server Running NetWare 6.5 SP3 or Later" on page 18	Added information about how to open and close a bash shell on a NetWare® server.