

Novell Open Enterprise Server

2

September, 2007

OPENWBEM SERVICES
ADMINISTRATION GUIDE

www.novell.com



Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright© 2005-2007 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see [the Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

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

This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

This product includes materials licensed under the Apache license, including Apache and Tomcat.

Contents

About This Guide	7
1 Overview	9
1.1 What's Next	10
2 What's New (OES 2 Initial Release)	11
3 Migrating OpenWBEM from NetWare to OES 2 Linux	13
3.1 Coexistence	13
3.1.1 Compatibility	13
3.1.2 Coexistence Issues	13
3.2 Migration	13
4 Running OpenWBEM in a Virtualized Environment	15
5 Setting Up OpenWBEM	17
5.1 Installing OpenWBEM	17
5.2 LUM-Enabling OpenWBEM During OES 2 Linux Installation	17
5.3 Starting, Stopping, or Checking Status for OWCIMOMD	17
5.4 Ensuring Secure Access	18
5.4.1 Certificates	18
5.4.2 Ports	19
5.4.3 Authentication	20
5.5 Setting Up Logging	21
5.5.1 Linux	21
5.5.2 NetWare	22
6 Changing the OpenWBEM CIMOM Configuration	23
6.1 Changing the Authentication Configuration	23
6.1.1 http_server.allow_local_authentication	24
6.1.2 http_server.digest_password_file	24
6.1.3 http_server.ssl_client_verification	25
6.1.4 http_server.ssl_trust_store	25
6.1.5 http_server.use_digest	26
6.1.6 owcimomd.ACL_superuser	26
6.1.7 owcimomd.allowed_anonymous	27
6.1.8 owcimomd.allowed_users	27
6.1.9 owcimomd.authentication_module	28
6.1.10 simple_auth.password_file	29
6.2 Changing the Certificate Configuration	30
6.3 Changing the Port Configuration	30
6.4 Changing the Default Logging Configuration	31
6.4.1 log.main.categories	31
6.4.2 log.main.components	32
6.4.3 log.main.format	33

6.4.4	log.main.level	34
6.4.5	log.main.location	35
6.4.6	log.main.max_backup_index	35
6.4.7	log.main.max_file_size	35
6.4.8	log.main.type	36
6.5	Configuring Debug Logging	36
6.5.1	Debug Log with Color	37
6.6	Configuring Additional Logs	37

7 Security Considerations 39

7.1	Secure Access	39
7.2	CIM Providers	39

About This Guide

This guide gives an overview of OpenWBEM services and Common Information Model (CIM) technologies included with Novell® Open Enterprise Server (OES) 2 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:

- ♦ Chapter 1, “Overview,” on page 9
- ♦ Chapter 2, “What’s New (OES 2 Initial Release),” on page 11
- ♦ Chapter 3, “Migrating OpenWBEM from NetWare to OES 2 Linux,” on page 13
- ♦ Chapter 4, “Running OpenWBEM in a Virtualized Environment,” on page 15
- ♦ Chapter 5, “Setting Up OpenWBEM,” on page 17
- ♦ Chapter 6, “Changing the OpenWBEM CIMOM Configuration,” on page 23
- ♦ Chapter 7, “Security Considerations,” on page 39

IMPORTANT: OES NetWare and NetWare 6.5 share the same code base and are the same in every way. Installing the OES NetWare product or associated support pack is the same as installing the simultaneously released NetWare 6.5 product or associated support pack.

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 *OES 2: OpenWBEM Services Administration Guide*, see the [Open Enterprise Server online documentation \(http://www.novell.com/documentation/oes2/cimom/data/front.html#bktitle\)](http://www.novell.com/documentation/oes2/cimom/data/front.html#bktitle).

Additional Documentation

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

For more information on the open source project OpenWBEM, see the [OpenWBEM Web site \(http://openwbem.org\)](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) 2 has embraced the open standard strategies of Web-Based Enterprise Management (WBEM) proposed by the [Distributed Management Task Force \(DMTF\)](http://www.dmtf.org/home) (<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 DMTF 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) (<http://openwbem.org>).

The packages contained in the Web-based Enterprise Management pattern in the Primary Functions category (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
Learn about coexistence and migration issues.	"Migrating OpenWBEM from NetWare to OES 2 Linux" on page 13
Setting Up OpenWBEM	"Setting Up OpenWBEM" on page 17
Learning about virtualization differences	"Running OpenWBEM in a Virtualized Environment" on page 15
Configuring OpenWBEM	"Changing the OpenWBEM CIMOM Configuration" on page 23
Ensure the server and data are secure	"Security Considerations" on page 39

What's New (OES 2 Initial Release)

2

OpenWBEM in Open Enterprise Server 2 includes the following features that were not in the initial release of OES 1:

- ♦ For OES Linux, OpenWBEM software packages are distributed by the SUSE® Linux Enterprise Server 10 software rather than added on by the OES software.
- ♦ The version of OpenWBEM for Linux is version 3.2. The version for NetWare® is still 3.01.

Migrating OpenWBEM from NetWare to OES 2 Linux

3

The section contains the following information:

- [Section 3.1, “Coexistence,” on page 13](#)
- [Section 3.2, “Migration,” on page 13](#)

3.1 Coexistence

This section provides information regarding the compatibility and coexistence of OpenWBEM Services with existing networks containing OES 2 NetWare® or Linux platforms.

3.1.1 Compatibility

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

Table 3-1 *Compatibility of OES Services using OpenWBEM Services on Various Versions of Operating Systems*

Operating System	Compatible Versions	Version of OpenWBEM
NetWare	OES 2 on NetWare	3.1
NetWare	OES 1 on NetWare	3.1
NetWare	NetWare 6.5 SP3 or later	3.1
Linux	OES 2 on Linux	3.2
Linux	OES 1 on Linux	3.1
Linux	SUSE® Linux Enterprise Server 9 SP1 and later	3.1
Linux	SUSE Linux Enterprise Server 10 and later	3.2

3.1.2 Coexistence Issues

Unknown.

3.2 Migration

When you migrate different OES 1 services from NetWare to OES 2 Linux, the services should automatically convert their use of OpenWBEM on NetWare version 3.1 to OpenWBEM on OES 2 Linux. You do not need to take any manual steps to make this conversion.

If you have modified the `openwbem.conf` file for your NetWare environment, you might want to make the same type of changes in the `openwbem.conf` file on Linux.

On OES Linux, the `openwbem.conf` file is the same name as it is for NetWare but file locations and settings are different, so you cannot copy the file directly from NetWare to an OES Linux server. The concepts are the same, so you can use the information from the NetWare `openwbem.conf` file to guide you in setting up the configuration on OES Linux. For all differences, see [“Changing the OpenWBEM CIMOM Configuration” on page 23](#).

Running OpenWBEM in a Virtualized Environment

4

OpenWBEM runs in a virtualized environment just as it does on a physical NetWare® server or on a physical server running OES 2 Linux and requires no special configuration or other changes.

To get started with virtualization, see “[Introduction to Xen Virtualization](#)” in the *Virtualization: Getting Started* guide.

For information on setting up virtualized NetWare, see “[Setting Up Virtual Machines](#)” in the *Virtualization: Getting Started* guide and “[NetWare Virtual Machines](#)” in the *Virtualization: Guest Operating System Guide*.

For information on setting up virtualized OES 2 Linux, see “[Setting Up Virtual Machines](#)” in the *Virtualization: Getting Started* guide and “[OES Linux Virtual Machines](#)” in the *Virtualization: Guest Operating System Guide*.

Setting Up OpenWBEM

5

This section includes the following information:

- ♦ [Section 5.1, “Installing OpenWBEM,” on page 17](#)
- ♦ [Section 5.2, “LUM-Enabling OpenWBEM During OES 2 Linux Installation,” on page 17](#)
- ♦ [Section 5.3, “Starting, Stopping, or Checking Status for OWCIMOMD,” on page 17](#)
- ♦ [Section 5.4, “Ensuring Secure Access,” on page 18](#)
- ♦ [Section 5.5, “Setting Up Logging,” on page 21](#)

5.1 Installing OpenWBEM

When you install or apply a support pack to Novell® Open Enterprise Server (OES) 2 on NetWare®, OpenWBEM is installed by default.

When you install any component of OES 2 on Linux that is dependent on OpenWBEM packages, the OpenWBEM packages from SLES 10 SP1 are installed automatically.

If you want to install only OpenWBEM, you only need to select the *Web-Based Enterprise Management* pattern from the *Primary Functions* category of the Software Selection page.

5.2 LUM-Enabling OpenWBEM During OES 2 Linux Installation

During the installation of OES 2 Linux or when adding OES 2 Linux on an existing server, ensure that you LUM-enable OpenWBEM when you are configuring LUM. This is the default setting.

If OpenWBEM is not LUM-enabled, the following services might not work as designed on an OES 2 Linux server:

- ♦ Novell iPrint
- ♦ Novell Remote Manager (NRM)
- ♦ Novell Samba
- ♦ Novell Storage Services™ (NSS)
- ♦ Storage Management Services™ (SMS)

5.3 Starting, Stopping, or Checking Status for OWCIMOMD

When OpenWBEM is installed, it installs and starts the OpenWBEM cimom daemon (OWCIMOMD) by default on OES on Linux and on OES on NetWare. Information in the following table explains how to start, stop, and check status for OWCIMOMD.

Table 5-1 *Commands for Managing OWCIMOMD*

Task	Linux Command	NetWare Command
Start OWCIMOMD	As root in a console shell, enter <code>rcowcimomd start</code> .	As user Admin or equivalent at the System Console, enter <code>openwbem</code> .
Stop OWCIMOMD	As root in a console shell, enter <code>rcowcimomd stop</code> .	As user Admin or equivalent at the System Console, enter <code>unload owcimomd</code> .
Check OWCIMOMD status	As root in a console shell, enter <code>rcowcimomd status</code> .	As user Admin or equivalent at the System Console, enter <code>modules owcimomd</code> . You can also view the list of loaded modules by using Novell Remote Manager. See “Managing Packages” in <i>OES 2: Novell Remote Manager Administration Guide for Linux</i> .

5.4 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.

- ♦ [Section 5.4.1, “Certificates,” on page 18](#)
- ♦ [Section 5.4.2, “Ports,” on page 19](#)
- ♦ [Section 5.4.3, “Authentication,” on page 20](#)

5.4.1 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 5-2 *Default Locations for Generated Certificates*

Platform	File Location
Linux	<code>/etc/openwbem/servercert.pem</code>
NetWare	<code>sys:/system/cimom/etc/openwbem/hostkey+cert.pem</code>

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 5-3 *Commands for Generating Certificates*

Platform	Command
Linux	As root in a console shell, enter <code>sh /etc/openwbem/owgencert.</code>
NetWare	As user Admin or with equivalent rights in a Bash console shell, enter: <code>/system/cimom/etc/openwbem/owgencert.</code> To get a bash prompt, enter <code>bash</code> at the System Console prompt. To exit the bash console shell, enter <code>exit</code> . For more information about using bash commands on NetWare, see “BASH” in the OES 2: Utilities Reference .

If you want to change the certificate that OpenWBEM uses, see “[Changing the Certificate Configuration](#)” on page 30.

5.4.2 Ports

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

Table 5-4 *Port Communication Setup and Recommended Configurations*

Port	Type	Notes and Recommendations
5989	Secure	<p>The secure port that OpenWBEM communications use via HTTPS services.</p> <p>This is the default configuration.</p> <p>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.</p> <p>Novell recommends that you maintain this setting in the configuration file.</p> <p>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.</p>
5988	Non-secure	<p>The non-secure port that OpenWBEM communications use via HTTP services.</p> <p>This setting is disabled by default.</p> <p>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.</p> <p>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.</p> <p>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.</p>

If you want to change the default port assignments, see [“Changing the Port Configuration” on page 30](#).

5.4.3 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 [“Changing the Authentication Configuration” on page 23](#).

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 LUM-enabled user can authenticate to the OpenWBEM CIMOM.
- ♦ If a 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.nlmldap_auth.ldap_host = 127.0.0.1ldap_auth.cert_file = /public/RootCert.der`

You need to reconfigure the LDAP settings as shown in the following table. To change these settings, see [“owcimomd.authentication_module” on page 28](#).

Table 5-5 *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 <code>public/RootCert.der</code> file on the local server to the <code>RootCert.der</code> file for the LDAP server in your network.
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 settings, 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 28](#).

5.5 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 31](#).

- ♦ [Section 5.5.1, “Linux,” on page 21](#)
- ♦ [Section 5.5.2, “NetWare,” on page 22](#)

5.5.1 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).

5.5.2 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\owmgmt_openwebem_lx_nwd.log` file. The default file size is 1000 KB with one backup file. It logs all errors for all components (OWCIMOMD).

Changing the OpenWBEM CIMOM Configuration

6

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 6-1 *Openwbem.conf File Locations*

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

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:

- ♦ [Section 6.1, “Changing the Authentication Configuration,” on page 23](#)
- ♦ [Section 6.2, “Changing the Certificate Configuration,” on page 30](#)
- ♦ [Section 6.3, “Changing the Port Configuration,” on page 30](#)
- ♦ [Section 6.4, “Changing the Default Logging Configuration,” on page 31](#)
- ♦ [Section 6.5, “Configuring Debug Logging,” on page 36](#)
- ♦ [Section 6.6, “Configuring Additional Logs,” on page 37](#)

6.1 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:

- ♦ [Section 6.1.1, “`http_server.allow_local_authentication`,” on page 24](#)
- ♦ [Section 6.1.2, “`http_server.digest_password_file`,” on page 24](#)
- ♦ [Section 6.1.3, “`http_server.ssl_client_verification`,” on page 25](#)
- ♦ [Section 6.1.4, “`http_server.ssl_trust_store`,” on page 25](#)

- ♦ [Section 6.1.5, “http_server.use_digest,” on page 26](#)
- ♦ [Section 6.1.6, “owcimomd.ACL_superuser,” on page 26](#)
- ♦ [Section 6.1.7, “owcimomd.allowed_anonymous,” on page 27](#)
- ♦ [Section 6.1.8, “owcimomd.allowed_users,” on page 27](#)
- ♦ [Section 6.1.9, “owcimomd.authentication_module,” on page 28](#)
- ♦ [Section 6.1.10, “simple_auth.password_file,” on page 29](#)

6.1.1 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 = true
```

6.1.2 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
```

6.1.3 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
```

6.1.4 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
```

6.1.5 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 OpenWBEM setting. However, in OES 2 Linux and NetWare this is set to false.

Example

```
http_server.use_digest = false
```

6.1.6 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
```

6.1.7 owcimomd.allowed_anonymous

Purpose

Enables or disables anonymous logins to owmgmt_openwebem_lx_nwd.

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
```

6.1.8 owcimomd.allowed_users

Purpose

Specifies a list of users who are allowed to access OWCIMOMD data.

Syntax

```
owcimomd.allowed_users = option
```

Option	Use
<i>username</i>	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
```

6.1.9 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 x86	/usr/lib/openwbem/authentication/libnovellauthentication.so
Linux 64	/usr/lib64/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 = /usr/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 6-2 Configuration Options for Additional LDAP Settings Recognized by OWCIMOM.NLM

Setting with Default	Configuration Options
<code>ldap_auth.bind_timelimit = 3</code>	Specifies the time (in seconds) that OWCIMOMD spends binding to LDAP as a given user.
<code>ldap_auth.binddn =</code> <code>anonymousldap_auth.bindpw = N/A</code>	<p>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:</p> <pre>ldap_auth.binddn cn=manager, dc=example, dc=com ldap_auth.bindpw=secret</pre>
<code>ldap_auth.ldap_port = 636</code>	If you change the secure port that LDAP is configured to, change this port number.
<code>ldap_auth.searchscope = sub</code>	<p>Options: sub, one</p> <p>sub: Sets the LDAP search to search the container specified in the <code>ldap_auth.searchbase</code> setting and all of its subcontainers.</p> <p>Example context:</p> <pre>o=example_company ou=provo ou=provo,ou=users ou=provo,ou=sales ou=provo,ou=engineers</pre> <p>For example, if the searchbase context were set to <code>ou=provo,o=example_company</code> and the searchscope were set to sub, then the Provo container and all its subcontainers would be searched.</p> <p>one: Sets the LDAP search to search only the container specified in the <code>ldap_auth.searchbase</code> setting.</p> <p>For example, if the searchbase context were set to <code>ou=users,ou=provo,o=example_company</code> and the searchscope were set to one, then only the Users container would be searched.</p>
<code>ldap_auth.search_timelimit = 10</code>	Specifies the amount of time (in seconds) that OWCIMOMD spends searching for a user in LDAP.
<code>ldap_auth.user_cachesize = 10</code>	Specifies the number of user authentication entries that are cached. Range: 0 to 1000 entries.

6.1.10 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
```

6.2 Changing the Certificate Configuration

The `http_server.SSL_cert` and the `http_server.SSL_key` settings specify the location of the file or files that contains the host's private key and the certificate that is used by OpenSSL for HTTPS communications.

The `.pem` file is located in the following default locations:

Table 6-3 *.pem File Locations*

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

Syntax

```
http_server.SSL_cert = path_filename
```

and

```
http_server.SSL_key = path_filename
```

Linux Example

```
http_server.SSL_cert = /etc/openwbem/servercert.pem
```

```
http_server.SSL_key = /etc/openwbem/serverkey.pem
```

NetWare Example

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

6.3 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
<i>Specific_port_number</i>	Specify the specific port for HTTP or HTTPS communications. For HTTP, the default port is 5988. For HTTPS, the default port is 5989.
-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
```

6.4 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:

- ♦ [Section 6.4.1, “log.main.categories,” on page 31](#)
- ♦ [Section 6.4.2, “log.main.components,” on page 32](#)
- ♦ [Section 6.4.3, “log.main.format,” on page 33](#)
- ♦ [Section 6.4.4, “log.main.level,” on page 34](#)
- ♦ [Section 6.4.5, “log.main.location,” on page 35](#)
- ♦ [Section 6.4.6, “log.main.max_backup_index,” on page 35](#)
- ♦ [Section 6.4.7, “log.main.max_file_size,” on page 35](#)
- ♦ [Section 6.4.8, “log.main.type,” on page 36](#)

If you want to set up debug logging, see [Section 6.5, “Configuring Debug Logging,” on page 36](#).

If you want to set up additional logs, see [Section 6.6, “Configuring Additional Logs,” on page 37](#).

6.4.1 log.main.categories

Purpose

Specifies the categories the log outputs.

Syntax

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

Option	Use
<i>category_name</i>	<p>Specifies the categories to be logged using a space delimited list.</p> <p>The categories used in OWCIMOMD are:</p> <ul style="list-style-type: none"> ♦ DEBUG ♦ ERROR ♦ FATAL ♦ INFO <p>For more information about these options, see “log.main.level” on page 34.</p> <p>If specified in this option, the predefined categories are not treated as levels, but as independent categories. No default is available; if a category is not set, no categories are logged and the log.main.level setting is used.</p>
*	<p>All categories are logged.</p> <p>This is the default setting.</p>

Example

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

6.4.2 log.main.components

Purpose

Specifies the components that the log outputs.

Syntax

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

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

Example

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

6.4.3 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	<p>Date</p> <p>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 ISO 8601 format is assumed.</p> <p>The only addition is %Q, which is the number of milliseconds.</p> <p>For more information about the date format specifiers, see the documentation for the strftime() function found in the <ctime> header.</p>
%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 that 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
```

6.4.4 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.
INFO	Logs all Info, Error, and Fatal error messages.

Example

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

6.4.5 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
```

6.4.6 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
<i>unsigned_integer_above_0</i>	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
```

6.4.7 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
<i>unsigned_integer_in_KB</i>	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
```

6.4.8 log.main.type

Purpose

Specifies the type of main log OWCIMOMD uses.

Syntax

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

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

Example

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

6.5 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`

6.5.1 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 6-4 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

6.6 Configuring Additional Logs

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

```
owcimomd.additional_logs = logname
```

Separate multiple log names with 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
```

Security Considerations

7

This section includes issues that you should consider when installing and configuring OpenWBEM services on a Novell® Open Enterprise Server (OES) 2 Linux server.

- ♦ [Section 7.1, “Secure Access,” on page 39](#)
- ♦ [Section 7.2, “CIM Providers,” on page 39](#)

7.1 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. See [“Ensuring Secure Access” on page 18](#).

7.2 CIM Providers

The OWCIMOMD process changes the fsuid (file system UID) of the threads as they execute provider code. However, these providers run in the same process space as OWCIMOMD, which runs as `root`. The fsuid change is done for convenience of the providers so that they can determine the access that a user has to the file system. This fsuid change provides only a minimal level of security. For security purposes, the providers should be considered as running as `root`.

IMPORTANT: Because CIM providers must run as root they should be monitored for attacks.

For example, look in syslog files to find odd patterns of behavior or malicious activity. In addition, if CIM or its providers do security logging, look at those log files as well.