



Avaya™ Operational Analyst

Release 6.1

Installation Planning and Prerequisites

585-248-118
Issue 1.0
August 2003
Compas ID 96430

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, anyone who is not a corporate employee, agent, subcontractor, or person working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Web site:

<http://www.avaya.com>

Select **Support**, then select **Escalation Lists**. This Web site includes telephone numbers for escalation within the United States. For escalation telephone numbers outside the United States, select **Global Escalation List**.

Providing telecommunications security

Telecommunications security (of voice, data, and video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or person working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Use (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including, but not limited to, human and data privacy, intellectual property, material assets, financial resources, labor costs, and legal costs).

Your responsibility for your company's telecommunications security

The final responsibility for securing both this system and its networked equipment rests with you, an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources, including, but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site:

<http://www.avaya.com/support>

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites and does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Trademarks

Avaya is a trademark of Avaya Inc.

All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Ordering information: Avaya Publications Center

Voice: +1-207-866-6701
1-800-457-1764 (Toll-free, U.S. and Canada only)

Fax: +1-207-626-7269
1-800-457-1764 (Toll-free, U.S. and Canada only)

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Manager

Web: <http://www.avayadocs.com>

E-mail: totalware@gwsmail.com

Order: Document No. 585-248-118, Issue 1.0
August 2003

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:

<http://www.avaya.com>

Select **Support**, then select **Escalation Lists**. This Web site includes telephone numbers for escalation within the United States. For escalation telephone numbers outside the United States, select **Global Escalation List**.

Avaya Training

Avaya provides training for Avaya Operational Analyst. For more information, contact Avaya University at:

Web site: http://www.avaya-learning.com/logon_form.asp

E-mail address: avaya.u.helpdesk@accenture.com

US telephone: 1-800-288-5327

Outside US telephone: +1-303-406-6089

Comments

To comment on this document, send e-mail to crminfodev@avaya.com.

Acknowledgment

This document was written by the CRM Information Development group.

**Avaya Operational Analyst
Release 6.1
Installation Planning and Prerequisites**

Contents

Preface	7
Product description	7
Intended users	8
Reasons for reissue	8
Organization	8
Related information	9
Introduction	11
Avaya OA components	12
The role of Avaya OA in a contact center	13
Planning checklist	14
Server and database planning	15
Avaya OA server machine configurations	16
Determining system size and configuration	21
Database and server machine considerations	22
General considerations	22
Historical database considerations	23
Historical server considerations	24
Real-time server considerations	25
Report server considerations	25
Avaya IC considerations	26
Avaya Business Advocate considerations	26
Avaya CMS considerations	27
Hardware requirements	29
Client PC minimum hardware requirements	29
Server machine hardware sizing	30
RAID configurations for server machines	30
Software requirements	31
Client software requirements	32
Server software requirements	33
Software required for the historical database and Historical subsystem servers	34
Historical subsystem coresident with the historical database	35
Historical subsystem not coresident with the historical database	36

Contents

Software required for Real-time servers	37
Software required for Report servers	38
Basic Report server	38
Advanced Report server	39
Software required for Source-CMS collection subsystem	40
Software required for Source-EC (Event Collector) collection subsystem	40
Software required for Source-EC Bridge (Event Collector Bridge) collection subsystem	41
Software considerations	42
Operating systems	42
Partitioning	43
Swap space	44
Web server software	44
Historical database software	45
DB2 limit on SQL statement length	46
Cognos software	49
TimesTen software	49
Java Run-time Environment	50
Virus scan software	50
Other software considerations	50
Time synchronization	51
Networking	51
Security	51
Installing the historical database software	53
Filegroup and tablespace sizing	55
Common filegroups or tablespaces (required with OA)	55
CMS filegroups or tablespaces (required with CMS tables)	55
Avaya IC filegroups or tablespaces (required with Avaya IC tables)	56
Database configurations	57
Sample historical database layout	58
Installing Microsoft SQL Server 2000 on Windows	60
Selecting a database configuration	60
Avaya OA with Avaya IC or CMS, and a back-end database	61
Avaya OA with Avaya IC or CMS, and a coresident database	62
Installing SQL Server 2000 Server and Client tools	63
Configuring SQL Server 2000	64
Creating an SQL Server 2000 back-end database	65
Installing Oracle 8i on Windows	68
Selecting a database configuration	68
Avaya OA with Avaya IC or CMS, and a back-end database	69
Avaya OA with Avaya IC or CMS, and a coresident database	70
Installing Oracle 8i database server software on Windows	71
Configuring an Oracle database instance on Windows	71
Creating Avaya OA tablespaces on Windows	72
Installing Oracle 8i database client software on Windows	73
Installing Oracle 9i on Windows	74
Selecting a database configuration	74
Avaya OA with CMS and a back-end database	75

Avaya OA with CMS and a coresident database	76
Installing Oracle 9i database server software on Windows	77
Configuring an Oracle database instance on Windows	78
Creating Avaya OA tablespaces on Windows	78
Installing Oracle 9i database client software on Windows	79
Installing Oracle 8i on Solaris	81
Selecting a database configuration	81
Avaya OA with Avaya IC or CMS, and a back-end database	82
Avaya OA with Avaya IC or CMS, and a coresident database	83
Installing Oracle 8i database server software on Solaris	84
Configuring an Oracle database instance on Solaris	84
Creating Avaya OA tablespaces on Solaris	85
Installing Oracle 8i database client software on Solaris	85
Installing Oracle 9i on Solaris	86
Selecting a database configuration	86
Avaya OA with CMS and a back-end database	87
Avaya OA with CMS and a coresident database	88
Installing Oracle 9i database server software on Solaris	89
Configuring an Oracle database instance on Solaris	89
Creating Avaya OA tablespaces on Solaris	90
Installing Oracle 9i database client on Solaris	90
Installing DB2 on AIX	91
Selecting a database configuration	92
Avaya OA with Avaya IC or CMS, and a back-end database	92
Avaya OA with Avaya IC or CMS, and a coresident database	93
Installing DB2 software and creating the database instance on AIX	94
Preparing for installation	94
Installing the database server software	95
Setting the DB2 registry values and environment	96
Configuring the database tunables	97
Manual configuration of Avaya OA tablespaces on DB2	99
Installing DB2 administration client software on AIX	100
Setting up the OS	100
Installing the DB2 administration client software and setting the database alias	101
Troubleshooting the installation	103
Creating users and setting OS parameters	105
Making changes on a Windows 2000 server	106
Creating user IDs and group IDs on Windows servers	106
Configuring Real-time subsystem locale settings on Windows	107
Making changes on a Solaris server	108
Creating user IDs and group IDs on Solaris servers	108
Configuring locale settings in Solaris	110
Configuring Real-time subsystem parameters	111
Configuring semaphores	111
Configuring message logging	112
Making changes on an AIX server	113
Creating user IDs and group IDs on AIX servers	113

Contents

Configuring message logging	114
Setting up Web servers	117
Installing the IIS Web server on Windows	118
Installing and configuring Sun ONE Web Server on a Solaris machine	119
Installing and configuring WebSphere on an AIX machine	121
Prerequisites	121
Path definitions	122
Installing WebSphere	122
Changing the administration port.	122
Configuring the server.	124
Starting WebSphere and the Administrative Console	124
Administering WebSphere to run as a non-root user	125
Configuring resource settings	125
Removing the default application	126
Changing file permissions.	127
Starting WebSphere	127
Changing the HTTP Server properties (optional)	128
Creating a secure login by enabling Global Security (optional)	129
Appendix A: Time synchronization.	131
An explanation of time synchronization	132
Need for time synchronization	132
Customer prerequisites	134
Service requirements	134
Recommendations	135
References	135
Configuration tips for Tardis time synchronization on Windows	136
Configuration tips for NTPD time synchronization on Solaris	138
Setting up an NTP infrastructure	139
NTP Security	140
Configuration tips for NTPD time synchronization on AIX	141
Appendix B: Networking	143
Enabling TCP/IP networking	144
Verifying DNS Resolution	145
Verifying DNS Resolution in Windows	146
Verifying DNS Resolution on Solaris	147
Verifying DNS resolution on AIX	148
Troubleshooting an Unresolved DNS Entry	149
Glossary	151
Index	153

Preface

Avaya Operational Analyst Release 6.1 Installation Planning and Prerequisites describes the installation planning and prerequisites that must be done before Avaya Operational Analyst (OA) is installed.

This section includes the following topics:

- [Product description](#) on page 7
- [Intended users](#) on page 8
- [Reasons for reissue](#) on page 8
- [Organization](#) on page 8
- [Related information](#) on page 9

Product description

Avaya OA allows businesses to perform operational reporting for a multimedia contact center, smoothly growing from single channel analysis, to full interaction, multi-channel analysis with a common data model and common user interfaces across the contact center systems.

Avaya OA is a required component of Avaya Interaction Center (Avaya IC), functioning as its operational data store and contact center performance analysis system. Avaya OA replaces and significantly upgrades the reporting capabilities of previous Avaya IC products.

Avaya OA is also an optional add-on to Avaya Call Management System (CMS) for extended, online historical data storage and multi-site analysis, receiving External Call History (ECH) data and historical interval data from up to 30 CMS servers and up to 240 ACDs.

Intended users

This information is intended for personnel that make planning and buying decisions for the customer, database administrators, system administrators, and other members of the IT team.

Reasons for reissue

This is the first issue of this information.

Organization

This documentation includes the following topics:

- [Introduction](#) on page 11 describes the components of OA and how these components operate in a contact center environment.
- [Server and database planning](#) on page 15 describes supported server configurations and provides information you must consider when planning an OA installation.
- [Hardware requirements](#) on page 29 gives the minimum requirements for server and client hardware.
- [Software requirements](#) on page 31 gives the requirements for server and client software.
- [Installing the historical database software](#) on page 53 presents information about how to install and set up the historical database for use with OA.
- [Creating users and setting OS parameters](#) on page 105 describes special parameters that must be set on the servers that support the OA software.
- [Setting up Web servers](#) on page 117 describes how the Web server software must be set up on the different server platforms.
- [Appendix A: Time synchronization](#) on page 131 provides requirements and information about time synchronization software.
- [Appendix B: Networking](#) on page 143 describes how to set up and test TCP/IP networking for the OA servers.

- [Glossary](#) on page 151 defines terms, including abbreviations and acronyms, used in this documentation.

Related information

The following table lists all of the Avaya OA information, both documents and online help systems:

Title	Number	Compas ID
<i>Avaya Operational Analyst Release 6.1 What's New in Operational Analyst R6.1</i>	585-248-401	96547
<i>Avaya Operational Analyst Release 6.1 Installation Planning and Prerequisites</i>	585-248-118	96430
<i>Avaya Operational Analyst Release 6.1 Installation and Configuration</i>	585-248-119	96431
<i>Avaya Operational Analyst Release 6.1 Maintenance and Troubleshooting</i>	585-248-120	96432
<i>Avaya Operational Analyst Release 6.1 Reports Reference</i>	585-248-506	96546
<i>Avaya Operational Analyst Release 6.1 Administration Client Online Help</i>	See Administration client help or library CD-ROM	
<i>Avaya Operational Analyst Release 6.1 Basic Reports Online Help</i>	See Report client help	
<i>Data Model Help</i>	See product CD-ROM	
<i>Security Guide</i>	See product CD-ROM	

The following table lists Avaya IC information that may be helpful:

Title	Number	Compas ID
<i>Avaya Interaction Center Release 6.1 Installation Planning and Prerequisites</i>	585-248-001	96781
<i>Avaya Interaction Center Release 6.1 Installation and Configuration</i>	585-248-102	96791
<i>Avaya Interaction Center Release 6.1 Business Advocate Configuration and Administration</i>	585-248-501	96821

The `release_notes.pdf` file contains the latest notes about installation of OA components. It is recommended that you read these notes before installation.

After installation, you can view the release notes at:

- `%PABASE%\doc\release_notes.pdf` (Windows)
- `$PABASE/doc/release_notes.pdf` (Solaris and AIX)

The default installation directories that represent `%PABASE%` and `$PABASE` are:

- `c:\Program Files\Avaya\BI` (Windows)
- `/export/home/biadmin/BI` (Solaris)
- `/home/biadmin/BI` (AIX)

The database operations explained in this document require the services of either a qualified database administrator or a systems integrator who possesses in-depth knowledge of database fundamentals and of the operating system. Some suggested reference materials include:

- For Oracle databases:
 - Oracle8i 8.1.7 Installation Guide for Windows
 - Oracle8i 8.1.7 Client Installation Guide for Windows
 - Oracle8i Administrator's Reference Release 3 (8.1.7) for Sun SPARC Solaris
 - Oracle8i Installation Guide Release 3 (8.1.7) for Sun SPARC Solaris
 - Oracle9i Database Installation Guide (Windows)
 - Oracle9i Client Installation Guide Release 2 (9.2.0.1.0) for Windows
 - Oracle9i Installation Guide Release 2 for UNIX Systems
 - Oracle9i Administrator's Reference for UNIX Systems
- For Microsoft SQL databases:
 - Microsoft SQL Server 2000 Books Online
 - Microsoft database documentation
- For DB2 databases, the DB2 documentation, which is available online after you install the database software.
- For TimesTen databases, the TimesTen documentation, which is available online after you install the Real-time subsystem. The documentation is copied to the following location:
 - `C:\TimesTen\TimesTen4.5\32\Doc` (Windows)
 - `$PABASE/TimesTen4.5/doc` (Solaris and AIX)

For detailed information about how to install operating system software, refer to the documentation that accompanies the operating system software.

■ ■ ■ ■ ■ ■

Introduction

Avaya Operational Analyst (OA) is designed to address the data collection and management needs of the Customer Relationship Management (CRM) marketplace with reliability, availability, and scalability. The underlying structure of OA is comprised of a set of modules that can be scaled and customized running in a Microsoft Windows, Sun Solaris, or IBM AIX environment.

Avaya OA allows businesses to perform operational reporting for a multimedia contact center, smoothly growing from single channel analysis, to full interaction, multi-channel analysis with a common data model and common user interfaces across the contact center systems.

Avaya OA is a required component of Avaya Interaction Center (Avaya IC), functioning as its operational data store and contact center performance analysis system. Avaya OA replaces and significantly upgrades the reporting capabilities of previous Avaya IC products.

Avaya OA is also an optional add-on to Avaya Call Management System (CMS) for extended, online historical data storage and multi-site analysis, receiving External Call History (ECH) data and historical interval data from up to 30 CMS servers and up to 240 ACDs.

This planning document should be used to prepare your site for installation of the OA software. The individual configuration of OA is highly application-dependent and should be reviewed with your Avaya representative.

Important:

The database operations used with Avaya OA require the services of either a qualified database administrator or a systems integrator who possesses an in-depth knowledge of database fundamentals on the installed operating system.

This section includes the following topics:

- [Avaya OA components](#) on page 12
- [The role of Avaya OA in a contact center](#) on page 13
- [Planning checklist](#) on page 14

Avaya OA components

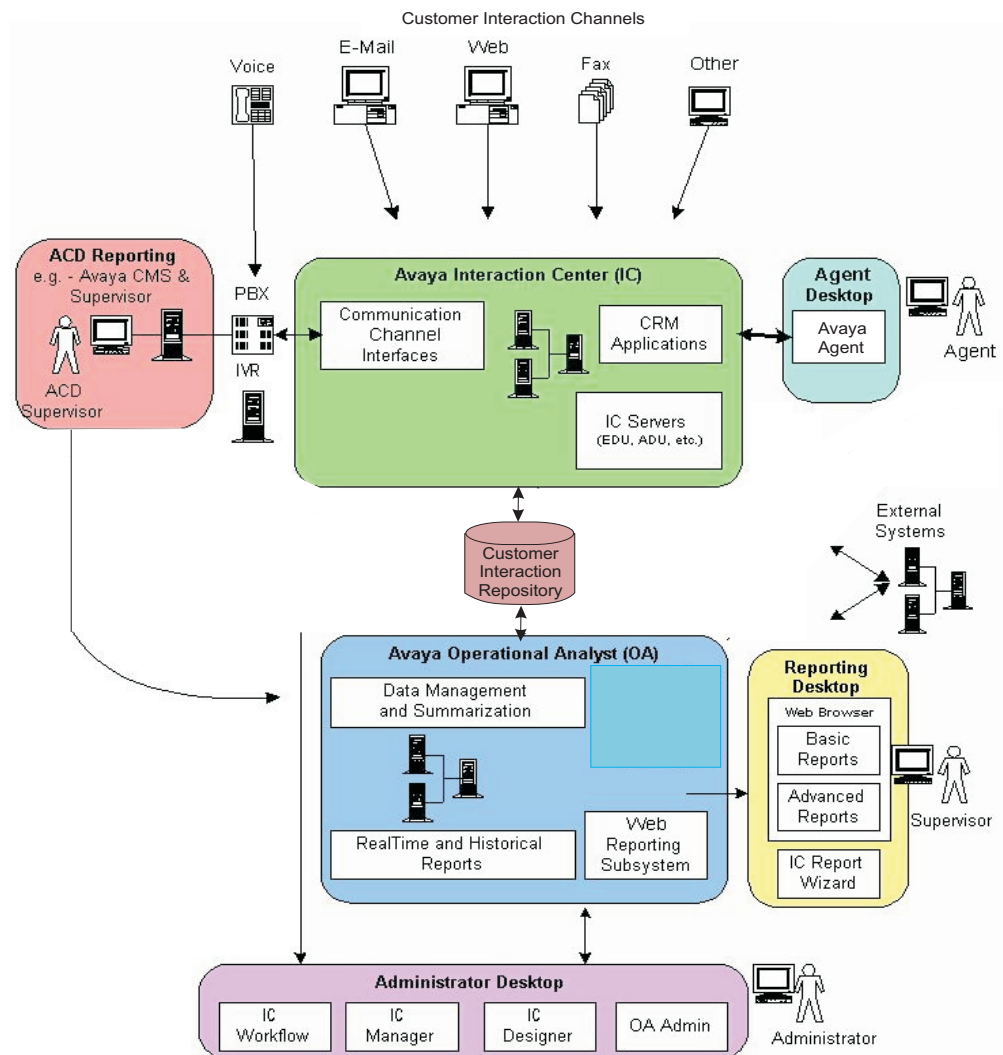
Avaya OA provides the following components:

- Integrated Avaya CRM logical data model of historical data for Avaya IC and Avaya CMS
- Integrated browser-based historical reporting across Avaya IC and Avaya CMS
- Improved real-time monitoring of data consistency and data presentation for Avaya IC
- Integrated browser-based real-time reporting for Avaya IC
- Pre-packaged summarization of Avaya IC data into the Customer Interaction Repository
- Pre-packaged data import facilities for all Avaya CMS External Call History and some CMS summary data into the Customer Interaction Repository
- Continued CMS operation, side by side with the Customer Interaction Repository, for voice-only customers without blending agents
- Multi-platform and multi-vendor support
- Multi-switch and multi-site support
- Internationalized code base with localized reports in several languages. For a complete list of supported languages, see your Avaya sales representative.

The role of Avaya OA in a contact center

Avaya OA provides business intelligence for the contact center. Avaya OA serves as the operational data store for customer interaction data, and as the contact center performance analysis system. Avaya OA provides:

- Data management and reporting for Avaya IC
- Integrated management and reporting for CMS
- Basic graphical and tabular (HTML) reports, viewed using a Web browser, for real-time and historical data
- Advanced analytical reports using third-party software from Cognos.



Planning checklist

To prepare your site for the installation of Avaya OA, use the procedures listed in the following checklist:

Procedure	✓
If your configuration includes Avaya IC, verify that all prerequisites have been done as described in <i>Avaya Interaction Center Release 6.1 Installation Planning and Prerequisites</i>. ⚠ Important: As you complete the Avaya IC prerequisites, some of the prerequisite items for Avaya OA detailed in this document (<i>Avaya Operational Analyst Release 6.1 Installation Planning and Prerequisites</i>) may be completed by prior work. Consult with your Avaya representative for assistance with installation prerequisites.	
See Server and database planning on page 15 to determine the number of server machines you must purchase to support your configuration.	
See Hardware requirements on page 29 to determine the hardware requirements for the server and client machines used to support your configuration.	
See Software requirements on page 31 to determine the software you must purchase and install to support your configuration. All third-party software must be installed on the server and client machines before you install the OA software.	
See Installing the historical database software on page 53 for instructions on how to install historical database software and configure the database to support OA.	
See Creating users and setting OS parameters on page 105 for instructions on how to configure parameters on the OS to support the OA components.	
See Setting up Web servers on page 117 for instructions on how to configure Web server software to support the OA components.	
If your configuration includes Avaya IC, install and configure Avaya IC as described in <i>Avaya Interaction Center Release 6.1 Installation and Configuration</i> .	
Install and configure OA as described in <i>Avaya Operational Analyst Release 6.1 Installation and Configuration</i> .	

■ ■ ■ ■ ■ ■

Server and database planning

Avaya OA is scalable to a wide range of work load specifications. Determine specific hardware sizing and installation procedures with assistance from the Avaya Professional Services Organization (PSO).

Avaya OA software operates on Microsoft Windows 2000 Server, Sun Solaris 8, or IBM AIX 5.1L. The OA software can run on a single server machine only for telephony applications in a small configuration (not recommended for a production system), or it can be distributed across multiple server machines in larger configurations (recommended configuration).

This section includes the following topics:

- [Avaya OA server machine configurations](#) on page 16
- [Determining system size and configuration](#) on page 21
- [Database and server machine considerations](#) on page 22

Avaya OA server machine configurations

Avaya OA consists of sets of subsystems and client software that are deployed on one or more machines (servers and client PCs). There are a number of supported configurations for the OA system, ranging from all subsystems and client software, except Avaya CMS, coresident on a single machine, to separate machines for each subsystem and client software. Because Avaya IC and OA support multi-site configurations, some of the subsystems and client software are deployed in multiple instances to support the multiple sites.

The configurations shown in this section are typical examples and do not show all possible configurations.



Important:

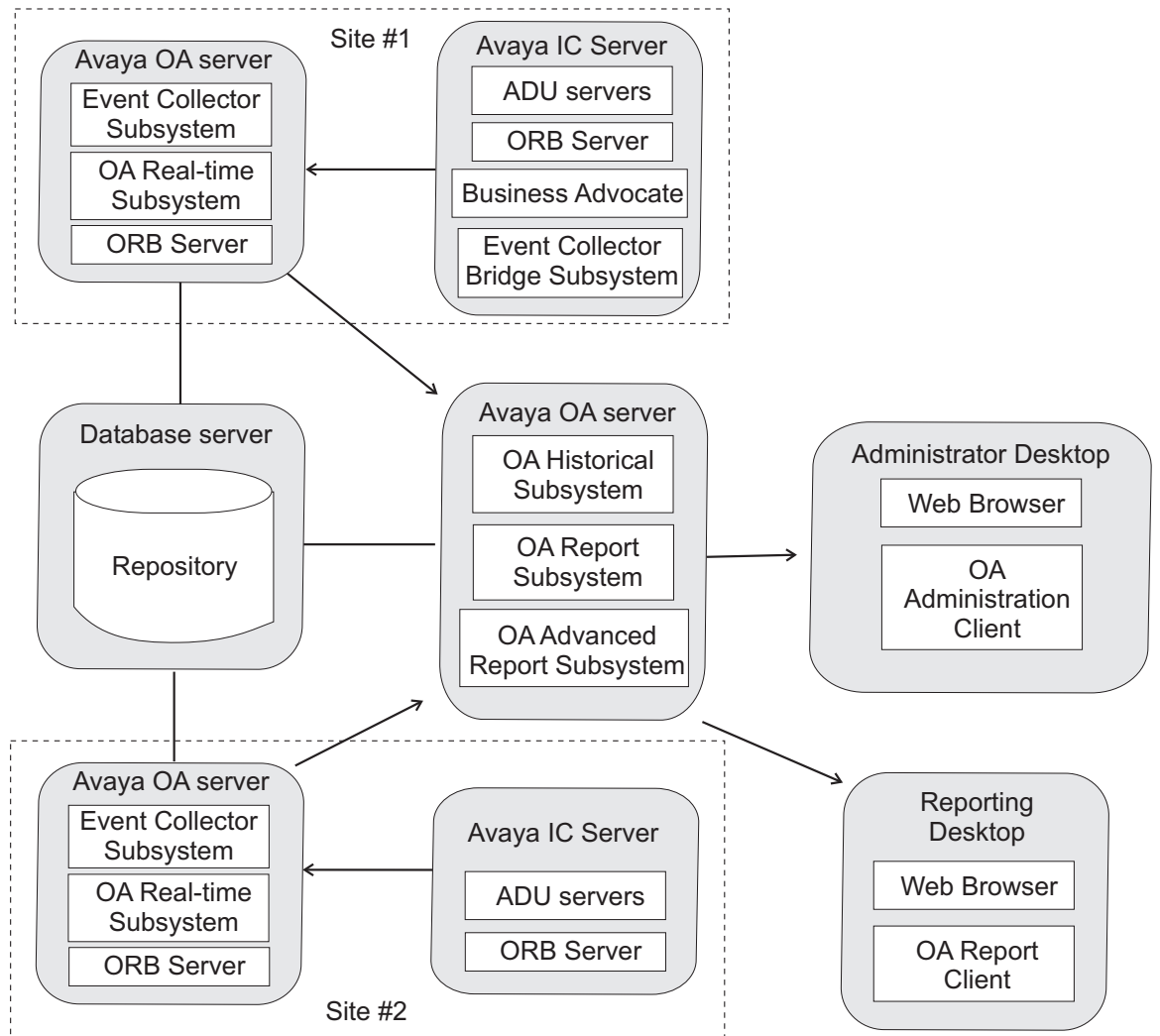
A single-machine configuration installed with Avaya IC subsystems, Avaya OA subsystems, and the historical database is recommended for a test system only. This configuration is not recommended for a production system.

Avaya recommends that you have a minimum configuration of three server machines; one for the installation of Avaya IC subsystems, one for the installation of Avaya OA subsystems, and one for the historical database.

Note:

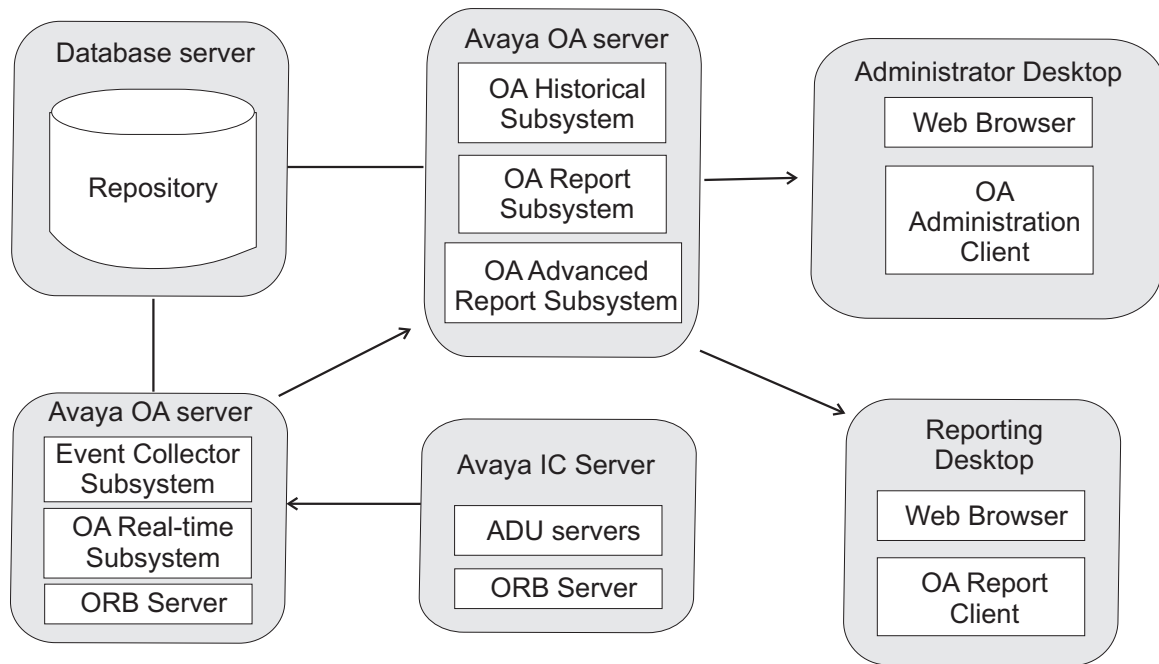
The diagrams in this section focus on Avaya OA servers, not Avaya IC servers. For more detailed configurations for Avaya IC servers, see *Avaya Interaction Center Release 6.1 Installation Planning and Prerequisites*.

The following figure illustrates a multi-site configuration with three OA server machines, a dedicated (back-end) historical database server machine, and several Avaya IC server machines (an actual configuration would show several more IC server machines).

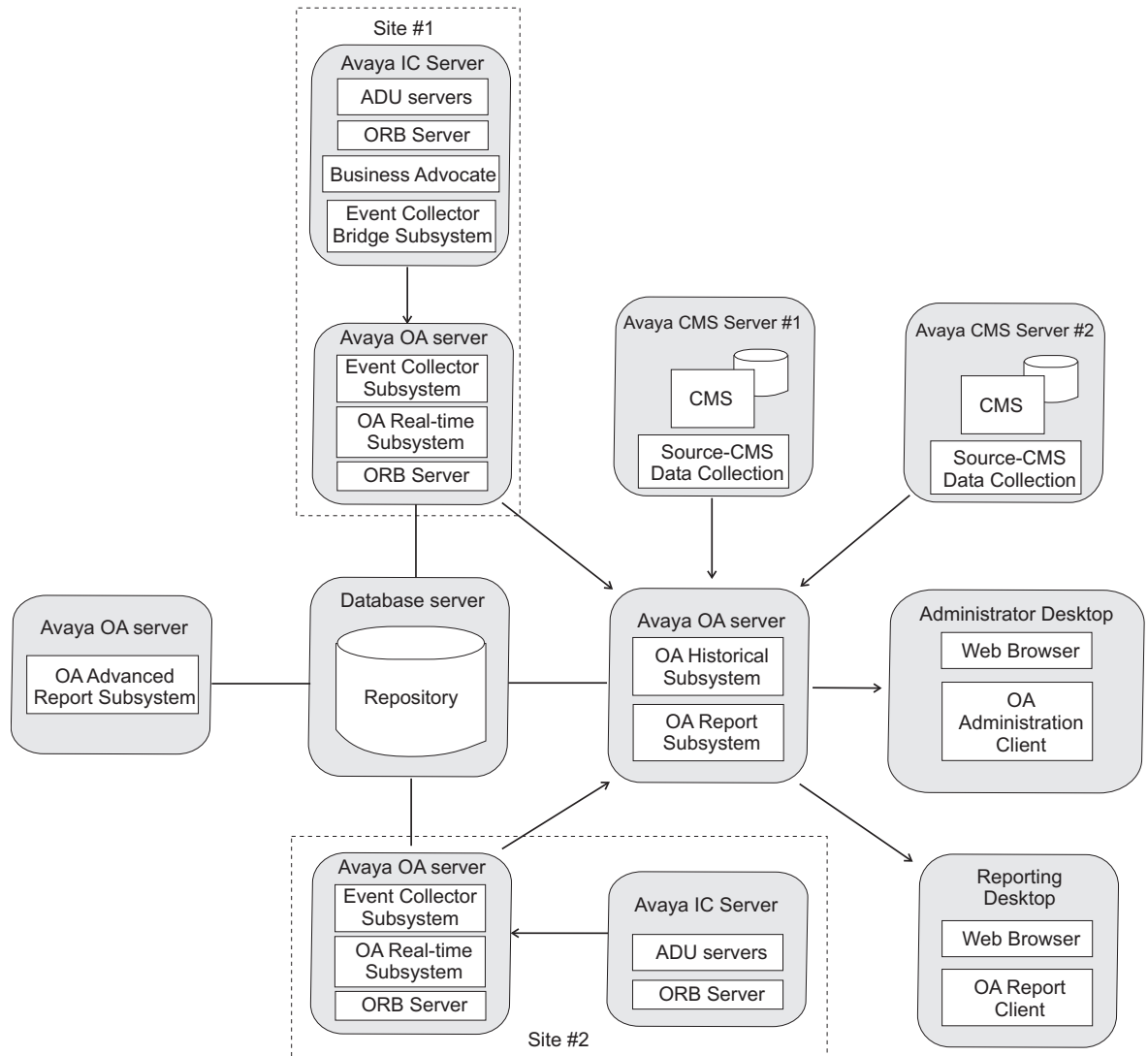


Server and database planning

The following figure illustrates a single-site configuration with two Avaya OA server machines, a dedicated (back-end) historical database server machine, and an IC server machine (an actual configuration would show several more IC server machines).

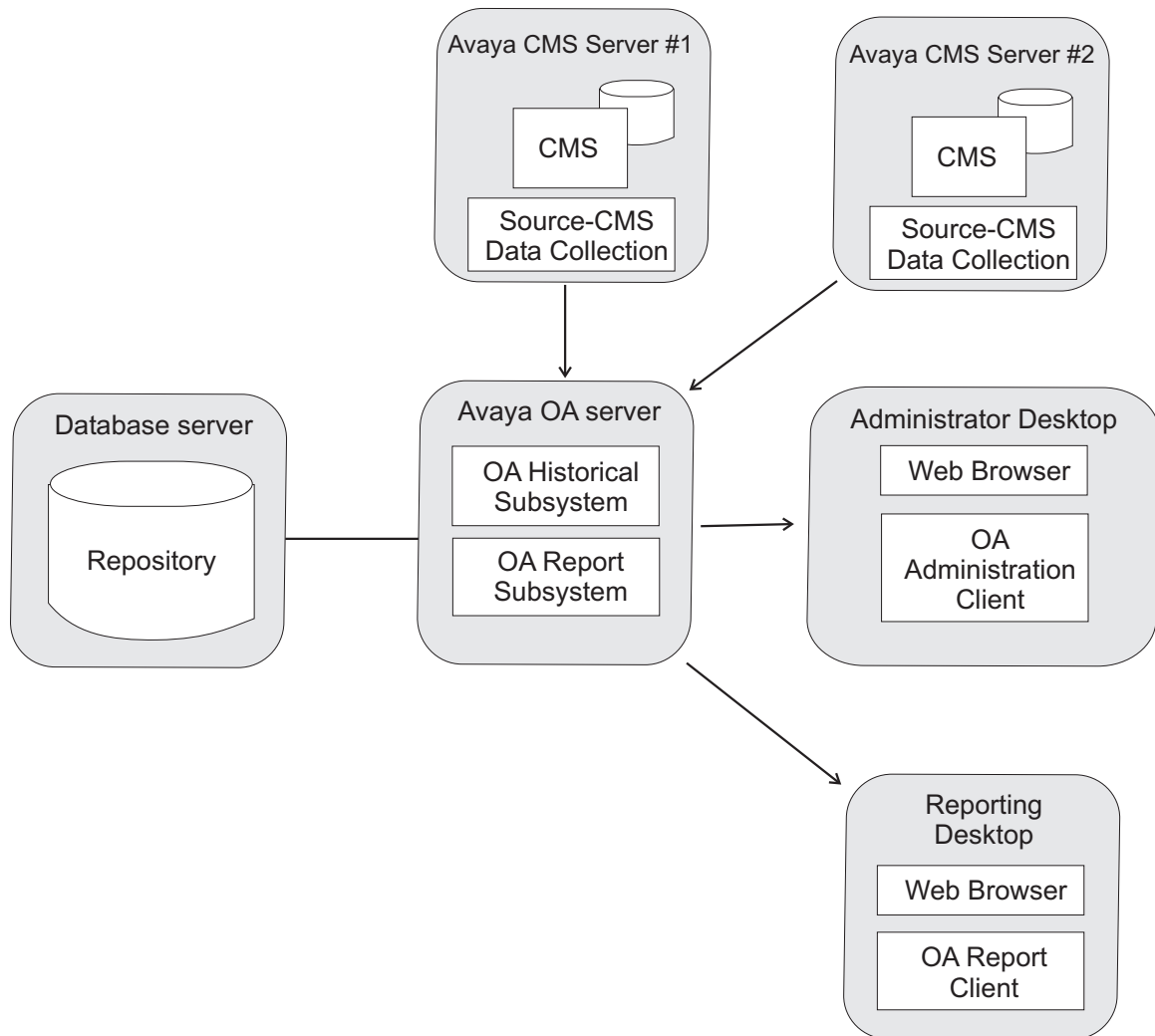


The following figure illustrates a multi-site configuration with four OA server machines (one machine dedicated for Cognos Advanced Reports), two CMS server machines, a dedicated (back-end) historical database server machine, and two Avaya IC server machines (an actual configuration would show several more IC server machines).



Server and database planning

The following figure illustrates a single-site configuration with an OA server machine, two CMS server machines, and a dedicated (back-end) historical database server machine.



Determining system size and configuration

The number of machines, the deployment of subsystems and client software among machines, and the amount of free disk space required are all factors that are influenced by the scope and activity of your business. It is very important that you estimate your projected future maximum performance and storage requirements before choosing a system configuration. The appropriate configuration for your system should be reviewed with your Avaya representative before making any purchasing decisions.

For example, a small business that receives data from only one type of customer contact, such as telephony, might be able to function with the one-machine configuration. This machine would house all of the OA components, including the databases, Administration client, and Report subsystem. This example assumes that the machine has enough space to store all real-time and historical data.

If more channels of customer contact (such as Web or e-mail) are added, a one-machine configuration could be quickly outgrown. In addition, modest storage space means that historical data must be archived to external storage media more frequently. A multi-machine configuration is recommended in this situation and for most business situations.

To help you more accurately determine your hardware requirements, consult the OA sizing tool available from Avaya PSO personnel.

Database and server machine considerations

Use the information in the following sections when planning an OA installation:

- [General considerations](#) on page 22
- [Historical database considerations](#) on page 23
- [Historical server considerations](#) on page 24
- [Real-time server considerations](#) on page 25
- [Report server considerations](#) on page 25
- [Avaya IC considerations](#) on page 26
- [Avaya Business Advocate considerations](#) on page 26
- [Avaya CMS considerations](#) on page 27

General considerations

For all servers used with OA, Avaya IC, and Avaya CMS configurations, consider the following issues:

CPUs - It is always better to have a server machine that has two (or more) CPUs, even at lower clock speeds, than a server with one CPU and double the clock rate. For example, a server machine that has two CPUs at 500 MHz generally outperforms a server machine that has one CPU at 1 GHz.

Planning for future growth - When selecting a server machine, plan for future growth when you choose storage space and CPU power. Do not try to squeeze your current Contact Center volumes into a machine that will be just big enough for now. Expect that you will expand in the future and will need more storage space and processing power.

Remote access for Avaya services - For server machines that require remote troubleshooting by Avaya, at least one Avaya machine in the customer network must have the following:

- A dial-up modem must be installed on a serial port.
- A phone line must be provided for the modem.
- Each Windows server that has a dial-up modem must have PCAnywhere installed on the server.

With a dial-up modem installed on at least one server in the customer network, Avaya services can gain access to most Avaya servers in the configuration. Avaya can also gain access using a customer's VPN, but that must be agreed to by the customer.

Historical database considerations

If you have a low activity or small historical database, the database can coreside on the same machine as the OA software. For all other configurations, Avaya recommends a separate database server machine (referred to as a back-end database server machine) for the OA and Avaya IC database instance. For large configurations, a Disk Storage Array may be necessary. It is very important to properly configure your database server machine to ensure good performance of your OA system. To determine the proper configuration for your database server machine, you must first consult with your Avaya PSO representative to get an estimate of the size and activity of your OA database. Your Avaya representative has a sizing tool for OA that will be used to determine the tablespace sizes and activity, which will help you determine the hardware configuration necessary for your OA database.

The hardware configuration of your database server machine will depend on the size and activity of your historical database. The general rule for setting up the database server machine is to spread high activity tables across as many disks as possible. Because OA is an update-intensive application, disk contention is a concern. If you configure many high activity tables onto a single large disk drive, the DataBase Management System (DBMS) will encounter disk contention for read/write access, and performance will suffer. The high activity tables need to be placed on separate disk drives to avoid the disk contention problem. Rollback segments and redo logs need to be placed on drives that are separate from high activity OA tables because the rollback segments and redo logs require a lot of disk input/output. These system resources need to have enough free disk space to allow for the worst case scenario of a large database operation. It is also necessary to make sure your OA tablespaces have enough space to fit the data you want to store. The OA sizing tool should give you the proper tablespace sizes for your configuration.

The specific layout of your OA tablespaces depends on the size and activity of the tablespace. Some general rules for grouping the OA tablespaces are given below. The high activity tablespaces for OA are typically:

- Avaya IC Inbound Contact tables: HISTICAGENT, HISTICAGENTSTATE, HISTICSCVSTATE, HISTICSVCCCLASS
- Avaya IC Outbound Contact tables: HISTICJOB, HISTICAGENTJOB, HISTICAGENTCOMP, HISTICSYSCOMP
- CMS tables: HISTCMSAGENT, HISTCMSCALLHIST, HISTCMSVDN, HISTCMSSKILL
- Status tables: HISTSTATUS
- DBMS system tables: vary by DBMS, but include Transaction Logs, Rollback Segments, Redo Logs, Temporary space

These tablespaces should be placed on separate disk drives to avoid disk contention. The number of elements of each data type (for example, agents) will determine the activity and size of the tablespace. For example, a configuration with only a few skills, but a lot of VDNs, would result in high database activity in the HISTCMSVDN tablespace, but low activity in the HISTCMSSKILL tablespace. For this example, you may put these

tablespaces on one disk drive. The high activity DBMS system tablespaces should always be separated from high-activity OA tables. The HISTSTATUS tablespace will always be a high activity tablespace and should be kept separate from the tablespaces with the highest activity (most elements).

In summary:

- Database performance is critical to OA performance and depends heavily on the hardware configuration and tablespace layout.
- A back-end database server machine should be used for all but the smallest configurations.
- The more disk drives the better (ideally, all high activity system and OA data should be on separate drives). Large configurations should consider a Redundant Array of Inexpensive Disks (see [RAID configurations for server machines](#) on page 30) or a Disk Storage Array.
- Group high activity tables together (on the same drive) with low activity tables.
- Consult with your Avaya representative to make sure your hardware configuration will be adequate and to help you design the tablespace layout for your configuration.

Historical server considerations

For implementations where OA is installed solely to collect CMS data, OA can be deployed in one-machine or two-machine configurations. The one-machine configuration hosts the OA software (Historical and Report subsystems) and the historical database. A one-machine configuration may be appropriate when the total call volume and number of agents across all CMS systems does not exceed 100,000 calls per day and 750 agents. If these capacities are exceeded, a two-machine configuration is recommended, with the OA software (Historical and Report subsystems) on one machine and the historical database on a second machine.

For implementations with Avaya IC and Avaya OA, Avaya recommends a multi-machine configuration. The historical database is shared by Avaya IC and OA software and should always be installed on a dedicated machine. The OA Historical and Report subsystems are generally installed on a second machine. Each Avaya IC site will have one or more Avaya IC server machines where the OA Event Collector and OA Real-time subsystems are installed.

Real-time server considerations

Avaya OA collects real-time events from Avaya IC through the Event Collector server, which is installed on an Avaya IC machine. Event Collector monitors one or more Agent Data Unit (ADU) servers for status about agents, queues, Business Advocate service classes, and Outbound Contact jobs. Each Event Collector is paired with a Real-time subsystem that summarizes events into a real-time database. The real-time database is used for real-time reporting and for transferring summarized data to the historical database for long term reporting.

Avaya recommends that a single Event Collector and Real-time subsystem should be installed and configured for each Avaya IC site. This Event Collector must be configured to monitor all of the agent ADU servers at this site. The Event Collector and Real-time subsystem should be installed together on the same Avaya IC machine.

If all the agent ADU servers at a site are located on a single machine, and if that machine has sufficient memory and processor speed, you can install the Event Collector and Real-time subsystem on that same machine, which will reduce LAN traffic. If the agent ADU servers at a site are located on multiple machines, you should install the Event Collector and Real-time subsystem on a machine that is different from the ADU servers.

For more information about deploying the Event Collector server to collect real-time data from Avaya IC, refer to *Avaya Interaction Center Release 6.1 Installation Planning and Prerequisites*.

The Real-time subsystem can be coresident with the Historical subsystem, the Report subsystem, or both the Historical and Report subsystems.

For implementations where OA is installed solely to collect CMS data, no Real-time subsystem or Event Collector is installed.

Report server considerations

The Report server is a Web server application that provides real-time and historical reports to supervisors and managers by using a Web browser. The Report server machine relies on commercial Web server software to provide Web access. Avaya OA provides both basic reporting and advanced reporting. An Advanced Report server machine requires installation of Cognos software before you install OA software.

The Report subsystem can be coresident on the same machine with the OA Real-time or Historical subsystems. In a multi-site environment, the Report subsystem should be installed on a machine at each site where supervisors run real-time reports.

In a large installation, you may need to install multiple Report server machines. A Report server can handle approximately 250 simultaneous real-time reports running at 30-second refresh rates. If the total number of real-time reports exceeds this capacity, you must install multiple Report server machines.

For multi-site implementations, an additional server machine for the OA Report subsystem should be installed at each site where there are 50 or more real-time report users.

 Important:

The Report subsystem cannot be coresident on a customer-facing Web server used for the Avaya IC Web channel. The Avaya IC Web components are typically available on the Internet outside your firewall, while the OA Report subsystem is typically available only inside your firewall. There are other Avaya IC components that use Web server technology such as the license manager, the Knowledge Base used by agents, and the e-mail letter generation capability used by supervisors and administrators. These components reside inside your firewall and can be coresident with the OA Report subsystem.

However, should any of Avaya IC components be coresident with the OA Report subsystem using Microsoft Internet Information Services (IIS) or if you have the IIS default Web site, a new Web site needs to be created for OA. Without a new Web site, both Avaya IC and OA Web server components use the default Web site of IIS. To resolve this conflict, see [Configuring IIS on Windows for coresident Avaya IC and Avaya OA](#) on page 101 in *Avaya Operational Analyst Release 6.1 Installation and Configuration*.

Note that creating a new Web site is not required when running Sun ONE Web Server on Solaris or when running WebSphere on AIX.

Avaya IC considerations

There are many considerations involved in designing a system where OA and Avaya IC functionality successfully works together. Refer to *Avaya Interaction Center Release 6.1 Installation Planning and Prerequisites* and your Avaya PSO representative for details.

Avaya Business Advocate considerations

If Avaya Business Advocate is included in the Avaya IC installation, at least one EC Bridge (Event Collector Bridge) subsystem must be installed. EC Bridge provides OA with Business Advocate administration data. The EC Bridge runs only on a Windows server with Avaya Business Advocate, and receives data from Business Advocate using Microsoft Message Queue (MSMQ).

Avaya recommends that one EC Bridge be deployed on each server where a Business Advocate Resource Manager is installed. If more than one EC Bridge is deployed, one EC Bridge serves as the primary EC Bridge while the other EC Bridges serve as standbys. If the primary EC Bridge fails, one of the standbys will take over and become the new primary EC Bridge.

Avaya CMS considerations

Avaya OA can collect historical data from up to 30 Avaya CMS server machines, which means data for up to 240 ACDs. Each CMS server machine must have the OA data collection software installed, the External Call History (ECH) feature purchased and enabled, and the ECH Handler program installed to successfully forward CMS data to OA. The OA data collection software serves as the link between the CMS and the historical database. If ECH is not purchased and enabled, the OA data collection software will not receive data from CMS.

Except for the data collection software that must be installed on each CMS server machine, OA software cannot be coresident with the CMS software.

Avaya OA requires the interval size on CMS to be set to 30 minutes. Avaya OA does not support 15-minute intervals.

Avaya OA requires that the CMS server have the latest generally available load of CMS. The specific CMS versions supported by OA at the time of publication are listed in the following table:

CMS version	Supported load and patch levels
R12	r3v12xx.x (to be determined)
R3V11	r3v11ag.b [QPPCN 1358B] Supplemental Services - ccsr9ac.a CMS Alarm Admin - AA9aa.j Visual Vector Server - vsv11aa.e Visual Vector Client - VV11F-01 CMS Supervisor - FJ.04 [QPPCN 1387B]
R3V9	r3v9aj.k patch issue 2 [QPPCN 1325B] Supplemental Services - ccsr9ac.a CMS Alarm Admin - AA9aa.i Visual Vector Server - vsv9b.a Visual Vector Client - VV9L.04 CMS Supervisor- EN.04 [QPPCN 1345B]

OA supports the following CMS hardware platforms:

- Sun Fire V880
- Sun Blade 100/150
- Sun Enterprise 3500
- Sun Ultra 5 (not supported in CMS R12)
- Sun Enterprise 3000 (not supported in CMS R12)

Server and database planning

The amount of memory (RAM) and free disk space required by the OA data collection software may exceed the amount available on the CMS server machine. Avaya OA requires 128 MB of memory and 2.5 GB of free disk space in a location other than root (/) in addition to the memory and disk space used by CMS. Specific requirements vary depending on ACD configuration. Consult the OA sizing tool available from Avaya PSO personnel to determine the amount required. Additional memory or disks may need to be purchased if the CMS does not have sufficient capacity. In general, a CMS with less than 384 MB of memory must be upgraded to support OA.

Hardware requirements

This section describes the minimum hardware required on client machines to install the OA client software and provides contact information where you can receive assistance when sizing servers for OA configurations.



Important:

These are *minimum* requirements. It is acceptable to use machines that are better than the minimum requirements.

This section includes the following topics:

- [Client PC minimum hardware requirements](#) on page 29
- [Server machine hardware sizing](#) on page 30
- [RAID configurations for server machines](#) on page 30

Client PC minimum hardware requirements

The minimum hardware requirements for a desktop PC running OA reports or using the Administration client are listed below:

Component	Minimum requirement
CPU	Intel-compatible 233 MHz
RAM	256 MB
Video	A graphics adapter capable of displaying 1024 x 768 pixels and 32,768 colors, with at least 8 MB of on-board RAM, and supporting 3D OpenGL acceleration. The latest driver version specifically issued for the video adapter (not the Microsoft version) must be used.
Virtual memory	700 MB allocated to the paging file
Free disk space	50 MB

Server machine hardware sizing

The OA server software can run on Windows 2000 Server machines, Solaris machines, or AIX machines. The hardware requirements for servers depend upon the deployment of an Avaya OA system, the volume of contacts in the contact center, and performance requirements. For assistance with sizing an OA configuration, contact your Avaya representative or Avaya Business Partner representative.

Note:

When OA-related software is being installed on Avaya IC machines, the machine must support the minimum requirements for Avaya IC as defined in *Avaya Interaction Center Release 6.1 Installation Planning and Prerequisites*.

RAID configurations for server machines

Redundant Array of Inexpensive Disks (RAID) uses multiple physical disks to implement one logical disk, as seen by the operating system. RAID configurations can consist of hardware only or a combination of hardware and software.

RAID provides an additional level of performance and fault tolerance. There are a number of common RAID configurations: RAID 0 (striping), RAID 1 (mirroring), and RAID 5 (striping with parity) are the most common configurations.

RAID 0, RAID 1, RAID 0+1, and RAID 5 are all acceptable configurations for OA when the Historical subsystem software is not coresident on the same machine with the historical database.

RAID 5 is not recommended for the historical database used with OA, which is an update-intensive application. RAID 5 tends to degrade write operations because the data and the parity must be read and then written with each update.



Software requirements

This section describes the software that must be installed on the client and server machines before you install the Avaya OA software.

This section includes the following topics:

- [Client software requirements](#) on page 32
- [Server software requirements](#) on page 33
- [Time synchronization](#) on page 51
- [Networking](#) on page 51
- [Security](#) on page 51

Client software requirements

The minimum software requirements for a desktop PC running OA reports or using the Administration client are listed in the following table:

Component	Minimum requirement
Operating system	Windows 2000 Professional, SP3 or Windows XP Professional (32-bit), SP1a or Windows NT ¹ 4.0 Workstation, SP6a
Web browser ²	Internet Explorer 6.0 SP1 or later
JRE	Java Runtime Environment 1.3.1_06 ³

1. Since Windows NT is an older operating system, you may find it difficult to upgrade video cards to the minimum hardware requirement and find the proper drivers to support the video cards in Windows NT. In this situation, Avaya recommends that you upgrade desktop computers that will run basic reports to Windows 2000 or Windows XP.
2. Internet Explorer is available from the Microsoft Web site: <http://www.microsoft.com>.
3. When you install the Administration client software, the JRE software is installed automatically. When you install the Report client support files, you are given the choice to install the JRE software if you do not already have the correct version.



CAUTION:

The Report client software must not be installed on an Avaya OA or Avaya IC server machine. Running reports on a server machine can adversely affect the performance of the server software.

Server software requirements

This section outlines the generic software requirements for OA components. Every effort was made to ensure that this information was complete and accurate at the time of publication. The actual installation steps for each software package may vary depending upon the version of the software media being used and other site-specific factors.

**Important:**

Avaya certifies support for the software versions documented in this section. Avaya will make an effort to support service packs that are guaranteed to be backwards compatible to the software versions shown in this section. Because this information is dependent upon third-party software, information is subject to change.

For an installation that includes Avaya IC and OA, OA processes and analyzes the data provided by Avaya IC. Therefore, you must install Avaya IC on your network before you install OA. In addition to Avaya IC, OA requires that other licensed (third-party) system-level software programs must be installed prior to installing OA. Avaya IC components and licensed system-level supporting software packages are available on separate distribution media. The OA distribution media includes internally developed components and associated software. All non-Avaya software, except that software noted in the tables that are bundled with OA software, must be purchased separately from OA software.

The following sections detail the OA software infrastructure required for each OA subsystem or client package. This information is intended only for reference. Deployment of software components may vary, depending on your system configuration and performance requirements. The version numbers associated with the supporting applications are specific to this release of OA.

This section includes the following topics:

- [Software required for the historical database and Historical subsystem servers](#) on page 34
- [Software required for Real-time servers](#) on page 37
- [Software required for Report servers](#) on page 38
- [Software required for Source-CMS collection subsystem](#) on page 40
- [Software required for Source-EC \(Event Collector\) collection subsystem](#) on page 40
- [Software required for Source-EC Bridge \(Event Collector Bridge\) collection subsystem](#) on page 41
- [Software considerations](#) on page 42

Software required for the historical database and Historical subsystem servers

The software required for machines with the historical database and the Historical subsystem depends on whether:

- the server machine has the historical database coresident on the same machine with the Historical subsystem ([Historical subsystem coresident with the historical database](#) on page 35), or
- the historical database is on a dedicated (back-end) machine and the Historical subsystem is on a separate machine with other OA software ([Historical subsystem not coresident with the historical database](#) on page 36).



Important:

The historical database cannot be coresident with any Avaya IC components. Only OA components, typically the Historical subsystem, are ever installed on the same server with the historical database.

Historical subsystem coresident with the historical database

The following table lists the software required on a server machine when the historical database is coresident on the same machine with the Historical subsystem:

Component	Windows	Solaris	AIX
Operating system	Windows 2000 Server with SP3 or Windows 2000 Advanced Server with SP3	Solaris 8	AIX 5.1L Maintenance Level 3 plus Patch IY34030
Time synchronization utility	NTP ¹	NTP ¹	NTP ¹
Historical database ²	Microsoft SQL Server 2000 SP3 (Standard or Enterprise Edition) or Oracle 8.1.7 Patch 4.0 (Standard or Enterprise Edition) or Oracle 9.2.0 Patch 1.0 ³ (Standard or Enterprise Edition)	Oracle 8.1.7 Patch 4.0 (Standard or Enterprise Edition) or Oracle 9.2.0 Patch 1.0 ³ (Standard or Enterprise Edition)	IBM DB2 7.2, FP9 Enterprise Edition (32-bit)

1. See [Time synchronization](#) on page 51 for more information.

2. See [Installing the historical database software](#) on page 53 for information about installing and configuring the database software.

3. Oracle 9i can be used in CMS standalone configurations, not in Avaya IC configurations.

Historical subsystem not coresident with the historical database

The following table lists the software required on a server machine when the historical database is not coresident on the same machine with the Historical subsystem (that is, the historical database is located on a dedicated, back-end database server machine):

Component	Windows	Solaris	AIX
Operating system	Windows 2000 Server with SP3 or Windows 2000 Advanced Server with SP3	Solaris 8	AIX 5.1L Maintenance Level 3 plus Patch IY34030
Time synchronization utility	NTP ¹	NTP ¹	NTP ¹
Historical database ²	Microsoft SQL Server 2000 SP3 client (Standard or Enterprise Edition) or Oracle 8.1.7 Patch 4.0 client or Oracle 9.2.0 Patch 1.0 ³ client (Standard or Enterprise Edition)	Oracle 8.1.7 Patch 4.0 client or Oracle 9.2.0 Patch 1.0 ³ client (Standard or Enterprise Edition)	IBM DB2 7.2, FP9 Enterprise Edition (32-bit)

1. See [Time synchronization](#) on page 51 for more information.

2. See [Installing the historical database software](#) on page 53 for information about installing and configuring the database software.

3. Oracle 9i can be used in CMS standalone configurations, not in Avaya IC configurations.

Software required for Real-time servers

The following table lists the software required on real-time server machines when using the Real-time subsystem:

Component	Windows	Solaris	AIX
Operating system	Windows 2000 Server with SP3 or Windows 2000 Advanced Server with SP3	Solaris 8	AIX 5.1L Maintenance Level 3 plus Patch IY34030
Time synchronization utility	NTP ¹	NTP ¹	NTP ¹
Real-time database	TimesTen 4.5.25 Real-time Database ² (bundled with OA software)	TimesTen 4.5.25 Real-time Database ² (bundled with OA software)	TimesTen 4.5.25 Real-time Database ² (bundled with OA software)

1. See [Time synchronization](#) on page 51 for more information.

2. If not present on the server machine, will be installed automatically when OA is installed. This software is installed in the same location as the OA software.

Software required for Report servers

This section provides the software required for Report server machines, both basic Report servers and Advanced Report servers.

This section includes the following topics:

- [Basic Report server](#) on page 38
- [Advanced Report server](#) on page 39

Basic Report server

The following table lists the software required on basic Report server machines when using the Report subsystem:

Component	Windows	Solaris	AIX
Operating system	Windows 2000 Server with SP3 or Windows 2000 Advanced Server with SP3	Solaris 8	AIX 5.1L Maintenance Level 3 plus Patch IY34030
Time synchronization utility	NTP ¹	NTP ¹	NTP ¹
Web server ²	Microsoft IIS 5.0 (installed when the OS is installed)	Sun One Web Server 6.0 SP5	IBM WebSphere 5.0.1, which includes IBM HTTP Server 1.3.26.1

1. See [Time synchronization](#) on page 51 for more information.

2. See [Setting up Web servers](#) on page 117 for more information.

Advanced Report server

The following table lists the software required on Advanced Report server machines when using the Advanced Report subsystem:

Note:

The Advanced Report subsystem can be installed only on machines with Windows server operating system. The Advanced Report subsystem is not supported on Solaris or AIX.

Component ¹	Windows
Operating system	Windows 2000 Server with SP3 or Windows 2000 Advanced Server with SP3
Browser (optional) ²	Internet Explorer 6.0 SP1 or later, or Netscape 4.76 or later
Cognos software ³	Cognos PowerPlay Transformation Server Version 7.0, MR1
	Cognos Impromptu Administrator Version 7.0, MR1 ⁴
	Cognos Impromptu Web Reports for Windows Version 7.0, MR1 (optional) ²
	Cognos PowerPlay Enterprise Server Version 7.0, MR1 (optional) ^{2 4}

1. This table shows the minimum requirements known at the time of publication for software used to support the Cognos software. For the latest requirements, see http://support.cognos.com/support/products/software_environments.html.

2. Required only when Web support is needed.

3. The Cognos software is shipped with the Avaya OA software on a separate CD-ROM.

4. To support multibyte report data in OA R6.1.1 for languages that are not supported by Impromptu Administrator Version 7.0, install the proper localized multibyte version of Impromptu Administrator Version 6.1. If the language you need is still not available in Version 6.1, install the multibyte English version. Note that Impromptu Administrator 6.1 will not support an Oracle 9i database.

Software required for Source-CMS collection subsystem

The following table lists the software required for Avaya CMS server machines (Solaris only) when OA is used to collect data from the CMS:

Component	Solaris
Operating system	Solaris 8

Software required for Source-EC (Event Collector) collection subsystem

The following table lists the software required when the Source-EC (Event Collector) subsystem is installed on an Avaya IC machine:

Component	Windows	Solaris	AIX
Operating system	Windows 2000 Server with SP3 or Windows 2000 Advanced Server with SP3	Solaris 8	AIX 5.1L Maintenance Level 3 plus Patch IY34030
Time synchronization utility	NTP ¹	NTP ¹	NTP ¹

1. See [Time synchronization](#) on page 51 for more information.

Software required for Source-EC Bridge (Event Collector Bridge) collection subsystem

The following table lists the software required when the Source-EC Bridge (Event Collector Bridge) subsystem is installed on an Avaya IC machine:

Note:

The Source-EC Bridge subsystem can only be installed on machines with Windows server operating system. The Source-EC Bridge is not supported on Solaris or AIX.

Component	Windows
Operating system	Windows 2000 Server with SP3 or Windows 2000 Advanced Server with SP3
XML parser	Microsoft XML Parser Version 3.0 SP1 or later ¹
Time synchronization utility	NTP ²

1. The required XML Parser is provided automatically when Internet Explorer 6.0 SP1 or later is installed on the server.

2. See [Time synchronization](#) on page 51 for more information.

Software considerations

This section describes issues you must consider when installing third-party software packages. Most third-party software packages are purchased separately and must be installed before you install OA.

Topics in this section include:

- [Operating systems](#) on page 42
- [Partitioning](#) on page 43
- [Swap space](#) on page 44
- [Web server software](#) on page 44
- [Historical database software](#) on page 45
- [DB2 limit on SQL statement length](#) on page 46
- [Cognos software](#) on page 49
- [TimesTen software](#) on page 49
- [Java Run-time Environment](#) on page 50
- [Virus scan software](#) on page 50
- [Other software considerations](#) on page 50

Operating systems

The server machines used with OA can operate with one or more of the following operating systems:

- Windows 2000 Server Service Pack 3 (minimum) or Advanced Server with Service Pack 3 (minimum)
- Solaris 8
- AIX 5.1L Maintenance Level 3 plus Patch IY34030

Windows 2000 requirements

There are no special requirements when installing Windows 2000.

Solaris 8 requirements

When installing Solaris, Sun recommends that you use the following strategy for applying patches:

- Install the recommended security patch cluster.
- Install any platform-specific hardware patches.

- Install any application-specific patches to applications used to support OA.

Note:

Depending on the configuration, Sun will not support hardware or software that has not been properly patched.

To avoid potential problems, you must install the latest Recommended Patch Cluster for Solaris 8 issued by Sun Microsystems. The latest Recommended Patch Cluster may include some of the required patches. Review the list of patches in the cluster before you install any additional patches.

You must install the latest versions of the patches for Solaris 8 shown in the following table:

Patch	Dependencies	Description
109147	None	Linker patch
108528	None	Security patch
108434-10	109147 from above	32-bit runtime patch for C++
108435-10	108434 from above	64-bit runtime patch for C++
111721	None	Math lib patch

To install the patches:

1. Download the patches from following website:

<http://www.sunsolve.sun.com/pub-cgi/show.pl?target=patchpage>

2. Follow the instructions provided by Sun Microsystems in the Readme file for the patch suite.

AIX requirements

When installing AIX, if you anticipate that your DB2 or TimesTen database will grow to more than 2 GB on an AIX filesystem, **Large File support** should be enabled for that filesystem. This must be done when you are creating the filesystem on an AIX machine. When you create the filesystem using `smitty`, you must choose **Add a Large File Enabled Journaled File System**.

Partitioning

Avaya recommends that the Web server logs and the TimesTen database be placed in their own respective partitions. Either of these can overflow and could cause other software sharing the given partition to fail. If each is stored on their own partition, they will be the only ones adversely affected by an overflow.

Software requirements

Swap space

For systems with 2 GB or less of memory (RAM), the paging file (Windows) or swap file (Solaris and AIX) should be set to 1 GB.

For systems with more than 2 GB of memory (RAM), the paging or swap file should be set to one-half the size of the memory (RAM).

Web server software

The Report subsystem requires a Web server software package. The following Web server software is supported, depending on the operating systems being used. For required software versions, see [Software required for Report servers](#) on page 38.

Windows 2000 - Microsoft IIS 5.0



Important:

The Report subsystem cannot be coresident on a customer-facing Web server used for the Avaya IC Web channel. The Avaya IC Web components are typically available on the Internet outside your firewall, while the OA Report subsystem is typically available only inside your firewall. There are other Avaya IC components that use Web server technology such as the license manager, the Knowledge Base used by agents, and the e-mail letter generation capability used by supervisors and administrators. These components reside inside your firewall and can be coresident with the OA Report subsystem.

However, should any of Avaya IC components be coresident with the OA Report subsystem using Microsoft Internet Information Services (IIS) or if you have the IIS default Web site, a new Web site needs to be created for OA. Without a new Web site, both Avaya IC and OA Web server components use the default Web site of IIS. To resolve this conflict, see [Configuring IIS on Windows for coresident Avaya IC and Avaya OA](#) on page 101 in *Avaya Operational Analyst Release 6.1 Installation and Configuration*.

Note that creating a new Web site is not required when running Sun ONE Web Server on Solaris or when running WebSphere on AIX.

Sun Solaris 8 - Sun ONE Web Server (formerly iPlanet) FastTrack and Enterprise Edition

AIX 5.1L - IBM WebSphere, which includes the IBM HTTP Server

Historical database software

Avaya OA supports the following software for the historical database:

- [Microsoft SQL Server 2000 Standard or Enterprise Edition](#) on page 45
- [Oracle Version 8i Standard or Enterprise Edition](#) on page 45
- [Oracle Version 9i Standard or Enterprise Edition](#) on page 45
- [IBM DB2 Enterprise Edition](#) on page 45

Microsoft SQL Server 2000 Standard or Enterprise Edition - SQL Server 2000 provides the database services needed by the Historical subsystem. [Installing the historical database software](#) on page 53 provides basic information about how to install SQL Server 2000 and set up an SQL Server 2000 database for OA. Details about the packaging and configuration of SQL Server 2000 are included in the SQL Server 2000 installation instructions. Specific customer configurations should be set up by a qualified database administrator.

Oracle Version 8i Standard or Enterprise Edition - Oracle provides the database services needed by the Historical subsystem. The determination of whether to use the Standard Edition or the Enterprise Edition is based on the expected size of your installation and your backup strategy. For smaller databases (50 to 85 GB), the backup capabilities of the Standard Edition are sufficient to allow use of this less expensive version. If you anticipate that your database will be larger than 85 GB, the Enterprise Edition allows you to take advantage of features like incremental backups.

Oracle Version 9i Standard or Enterprise Edition - Oracle provides the database services needed by the Historical subsystem. Oracle 9i supports only an OA and CMS configuration. Oracle 9i does not support an Avaya IC configuration. The determination of whether to use the Standard Edition or the Enterprise Edition is based on the expected size of your installation and your backup strategy. For smaller databases (50 to 85 GB), the backup capabilities of the Standard Edition are sufficient to allow use of this less expensive version. If you anticipate that your database will be larger than 85 GB, the Enterprise Edition allows you to take advantage of features like incremental backups.

IBM DB2 Enterprise Edition - DB2 provides the database services needed by the Historical subsystem and is required on the server machine where the Historical subsystem is present or on a back-end database configuration. Install the Enterprise Edition (32-bit).

DB2 limit on SQL statement length

A large percentage of OA customers who use the DB2 database and make use of OA containers with basic historical reports are likely to experience a problem stemming from a limitation of the DB2 database. The nature of the limitation is that DB2 imposes a limit on the maximum length of SQL statements that it will accept. It is a fixed limit that cannot be tuned or adjusted.

OA customers impacted will see the problem as an inability to successfully aggregate their OA container data. This aggregation failure in turn affects historical reports that access aggregated data since the needed aggregated data is unavailable.

Note:

This limitation does not apply to Oracle or to Microsoft SQL databases; it only applies to the DB2 database. Workarounds to lessen this limitation will be provided in future OA software updates. However, the final solution to the problem likely will depend on the DB2 limit being substantially increased or removed by IBM. This issue does not affect advanced historical reports or basic Real-time reports.

After reading this information and understanding the constraints imposed by the DB2 problem, OA customers should decide whether the constraints on this OA release are acceptable. If the constraints are not acceptable, the customer may want to use one of the other supported databases (SQL or Oracle), or plan to use DB2 in a future release of OA in which the DB2 limitations will be lessened.

Background - OA saves interval data into predefined data stores in the historical database. These data stores are specific to one or a combination of system objects such as agents, service classes, skills, jobs, and so on. Customers may define groupings of data within each of the data stores; these data groupings are called containers. Containers allow customers to group data in ways that are logical or convenient to them for reporting purposes. Container examples include grouping agents into separate containers by department or workgroup, or grouping related service classes or skills into separate containers. The OA aggregation process operates on the container data; it creates and executes SQL statements that process data for the defined containers into daily, weekly, and monthly periods for use in OA historical reporting. This aggregated data improves reporting usefulness, performance, and efficiency.

The greatest factors contributing to the length of aggregation SQL statements are:

- The number of system objects that are defined for a given container (customer controllable)
- Which data store the container is associated with (pre-defined by system)

Considering these factors, the larger the number of objects that are defined in a container, the longer the SQL statement must be to account for the defined objects. If the length of the SQL statement required to aggregate the data exceeds the DB2 limit, aggregation will fail and reporting will be impacted.

Note:

The amount of data in the database does not contribute to this problem.

Customer impact and selected analysis results - The DB2 SQL length limit is more likely to affect aggregation for some containers than others, depending on the specifics of the SQL statement required for the aggregation of each container's data. To assess the likelihood of customer impact, an analysis of the problem has been done using estimates of how typical customers configure their systems. The analysis shows that the likelihood of impact is greatest for containers in the IC and CMS agent stores and the CMS VDN store. More information is provided next for the most constraining cases for these stores.

- **IC Agents:** The constraints for the IC Agent store are most severe. Based on expected typical usage, the analysis shows that if a customer defines 20 service classes in a container, they are limited to between 36 agents (if English language) and 27 agents (if multi-byte language) in that container. If the number of either of these objects (agents or service classes) per container is increased, the number of the other object must be decreased. For example, if instead of 20 service classes the customer defines 30 service classes in a container, the number of allowable agents in that container decreases to between 24 agents (if English language) and 18 agents (if multi-byte languages). This is fewer than the expected number of IC agents a typical OA customer is expected to want to define per container.
- **CMS Agents:** The constraints for the CMSAgent store are slightly less severe than for the IC Agent store. For the OA CMSAgent store, the analysis shows that if a customer defines 25 splits from a single source (single ACD), they are limited to between 42 agents (if English language) and 39 agents (if multi-byte language). If either the number of splits or the number of sources per container is increased, the number of agents must be decreased. For example, if instead of 25 splits the customer defines 50 splits from a single source, the number of allowable agents in that container decreases to between 21 agents (English language) and 20 agents (multi-byte languages). Similarly, if the number of sources is increased to 2, with 25 splits, the number of allowable agents in that container again decreases to between 21 agents (English language) and 20 agents (multi-byte languages). This is fewer than the expected number of CMS agents a typical OA customer is expected to want to define per container.
- **For the CMS VDN store,** the analysis shows that if a customer defines VDN containers to be independent of data source, they can have approximately 3000 VDNs in that container. This is expected to be acceptable to the typical customer. If the VDN container is defined to have data from only a single data source, the number of allowable VDNs drops to approximately 1600. If the container is defined to have 2 data sources, the number of allowable VDNs drops to approximately 750. These last 2 examples illustrate cases where fewer VDNs are allowable than a typical customer is expected to want to define per container.

Guidelines for Customers - As stated above, customers can control one of the major factors that contribute to SQL statement length, namely, how many system objects are defined per container. As a general statement, the fewer system objects defined per container, the less likely the customer is to encounter the SQL length limit and have aggregation problems. This was illustrated for agents and VDNs in the analysis results described above.

The constraints imposed by the DB2 SQL limit may or may not be acceptable to a given customer. Each customer should consider the most constraining cases described above and compare them to their expected configuration (in the time frame of this OA release) to determine acceptability. If they are not acceptable, the alternative is to use a different OA-supported database.

The following guidelines are intended to provide customers some guidance on how to minimize the chance they will encounter the DB2 SQL length limit problem. These measures do not resolve the problem; they are work-around actions customers can take to help mitigate the problem. Be cautioned that they may not work in all cases, since they are based on estimates for a hypothetical typical customer.

- The general rule, if the DB2 SQL length problem is encountered, is to redefine containers to include all objects (other than agents) when possible, or alternately to include a smaller number of objects. Either of these techniques will reduce the SQL statement length.
- For CMS containers, define them so they are independent of the data source, that is, they hold data for the defined objects from all data sources. This will maximize the number of objects allowed per container. As an example of this for VDNs, define VDN containers so they are independent of the data source (holding data for the defined VDNs from all data sources).
- If it is not acceptable to define CMS containers independent of data source, next best is to define each container to have data from only a single source. This implies defining more containers, each with data from a single source. As an example of this for VDN containers, define each container to have data from only a single source.
- If CMS containers must contain data from multiple data sources, limit the number of other objects defined per container. This implies defining more containers, each with fewer objects. As an example of this for VDN containers, limit the number of VDNs defined per container.
- Similarly, for CMS container definitions with rules based on VDNs, CWCs, or Splits, it is beneficial to either:
 - define the container to include all VDNs, CWCs or Splits when that satisfies the customer need, or
 - reduce the numbers of VDNs, CWCs or Splits in the container definition. This implies defining more containers, each with a narrower scope of data.
- In IC agent containers, define them to include all dialers or service classes if possible. This will maximize the number of agents allowed per container.

- If it is not acceptable to include all dialers or service classes, then minimize the number of service classes, dialers and jobs defined per container. This will also increase the number of allowable agents. Use the above analysis results as a guideline. This implies defining more containers, each with a narrower scope of data.
- For both IC and CMS agent containers, if the preceding guidelines are not sufficient, limit the number of agents defined per container, using the above analysis results as a guideline. This again implies defining more containers, each with fewer agents.
- For IC containers other than for agents, a general statement for those that contain more than one object type is that minimizing the number of one of the object types will allow maximizing the other object type. For example, in Job and SysComp containers, minimizing the number of dialers defined per container will allow more jobs to be defined per container.
- Another potential option exists, that of reporting on unaggregated data. However, this is not thought to be a very useful option for customers because the time scale of all historical reports will be one-half hour intervals. This means that rather than seeing historical data summarized on a report by day, or week, or month, it will be presented by the half hour (base interval). For example, to see data for a 24-hour day, data for each of 48 half-hour intervals will be shown. This amount of data will clutter the report and make it very hard to interpret, spot historical trends, etc. Again, this will not be a viable option for the vast majority of customers, and perhaps none.

Cognos software

Avaya recommends that you install the Cognos software before you install the OA software. Also, if the server where the Cognos software is installed is using LDAP, the LDAP software must be installed before the Cognos software.

TimesTen software

When the Real-time subsystem is selected for installation, OA automatically installs the TimesTen software on the server machine.

Java Run-time Environment

Every OA server machine and client machine requires the Java Run-time Environment (JRE), which is installed automatically on the OA server machines and on the OA Administration client. The versions installed are as follows:

- Version 1.3.1_06 (Windows and Solaris)
- Version 1.3.1_01 (Solaris, only used by Stumbras on Report servers, but installed on all servers)
- 1.3.1 (AIX)

These are the only acceptable versions.

Note:

When OA installs JRE on a Windows server machine, the path environment is changed to place JRE first in the path. This could cause problems with other applications that depend on a different version of JRE.

Virus scan software

Virus scanning software can affect performance of OA. Make sure virus scanning is configured to scan program files only (that is, executables, DLLs, and so on), not *all* files. If virus scanning is configured to scan all files, OA performance may be unacceptable due to frequent scanning of log files and data files.

Avaya recommends virus scanning software be configured as follows:

- Scan only program and executable files, not all files.
- Exclude the directory %PABASE%\data from virus scanning.
- Exclude the directory %AVAYA_IC61_HOME%\logs from virus scanning.
- Configure full system scan to run when overall system activity is low.

Other software considerations

When the server machine uses other software and security packages, there is no guarantee that OA will operate properly. Avaya recommends that you do not run additional software on the OA server machines. The following is a list of software that has not been officially tested to work with OA and may or may not work when installed on an OA server:

- VMWARE
- Citrix
- Tivoli
- TACF
- Veritas Backup Exec

Time synchronization

Time synchronization is the process of ensuring that the time-of-day clocks of all server machines within a defined network are set to the same time. It is critical that the clocks maintain an accuracy of 0.5 seconds or better. If clock synchronization is not used:

- Report data will be missing or inaccurate.
- Agent and queue or service class interval counts may not match if the related timestamps do not match.
- If events are received out of order as a result of not having time synchronization, data may not be available for reporting, or negative durations may be computed.

If you already have a time synchronization infrastructure that meets the requirements for OA, have your system administrator include the OA server machines in that framework.

 CAUTION:

Batch scripts that periodically set the time, or tools like Windows Time Service, are not accurate enough for the historical database.

If you do not have an existing infrastructure, install NTP (Network Time Protocol) software on all server machines. For more information about NTP, see [Appendix A: Time synchronization](#) on page 131.

Networking

Your network must be configured properly so that the server machines communicate with each other. For more information about networking, see [Appendix B: Networking](#) on page 143.

Security

Avaya OA does not provide separate security. Security on all systems is maintained using security services provided by the operating system. Make sure all the accounts you use for installing, running, and administering OA have security settings that meet those required by your company. For more information on OA security, refer to Operational Analyst Security Guidelines, which is provided on the installation CD-ROM in the `docs` folder or directory.

Installing the historical database software

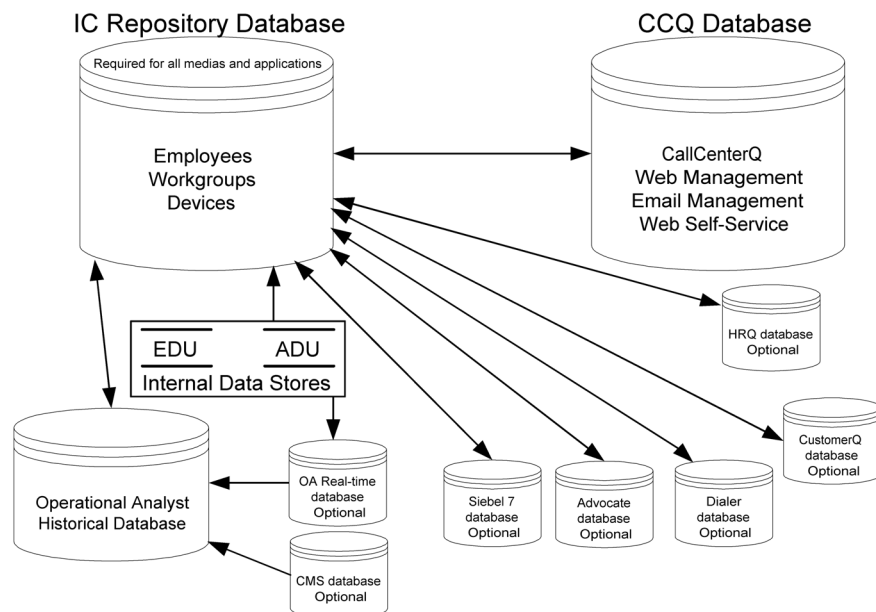
This section provides general information about installing and configuring the historical database. No one database layout is recommended. When needed, modify the steps based on your individual system requirements.

Important:

The database operations used with Avaya OA require the services of either a qualified database administrator or a systems integrator who possesses an in-depth knowledge of database fundamentals on the installed operating system. It should not be done by personnel that are not familiar with the database software.

A single historical database instance, installed only once on one server machine, is shared by the Avaya IC, CMS, and OA systems. You can refer to this document or to Avaya IC documents for instructions to install the database software and create the shared database instance. You should refer to Avaya IC documents for instructions on using Avaya Database Designer to configure the database.

This illustration shows how Avaya IC data, CMS data, and OA data share the same database instance but different tables:



Installing the historical database software

Whichever product you choose to install as your database, consult the documentation from the manufacturer for more information about how to install and set up your database.

This section includes the following topics:

- [Filegroup and tablespace sizing](#) on page 55
- [Database configurations](#) on page 57
- [Sample historical database layout](#) on page 58
- [Installing Microsoft SQL Server 2000 on Windows](#) on page 60
- [Installing Oracle 8i on Windows](#) on page 68
- [Installing Oracle 9i on Windows](#) on page 74
- [Installing Oracle 8i on Solaris](#) on page 81
- [Installing Oracle 9i on Solaris](#) on page 86
- [Installing DB2 on AIX](#) on page 91

Filegroup and tablespace sizing

There are three categories of filegroups (SQL Server 2000) or tablespaces (Oracle and DB2) in the database. The following sections list the names and minimum sizes of each category of filegroups or tablespaces:

- [Common filegroups or tablespaces \(required with OA\)](#) on page 55
- [CMS filegroups or tablespaces \(required with CMS tables\)](#) on page 55
- [Avaya IC filegroups or tablespaces \(required with Avaya IC tables\)](#) on page 56

Any changes to the amount of space allocated to the filegroups and tablespaces must be determined by the database administrator.

Common filegroups or tablespaces (required with OA)

Name	Minimum size (MB)
HISTADMIN	200
HISTSTATUS	300
HISTIDMAP	10

CMS filegroups or tablespaces (required with CMS tables)

Name	Minimum size (MB)
HISTCMSAGENT	500
HISTCMSCWC	50
HISTCMSSKILL	300
HISTCMSVDN	200
HISTCMSCALLHIST	500
HISTCMSSYNONYM	10

Avaya IC filegroups or tablespaces (required with Avaya IC tables)

Name	Minimum size (MB)
HISTICAGENT	100
HISTICAGENTSTATE	50
HISTICSVCCLASS	100
HISTICSVCSTATE	100
HISTICDISPLAY	25
HISTICAGENTCOMP	50
HISTICAGENTJOB	50
HISTICJOB	25
HISTICSYSCOMP	25

Database configurations

There are three possible database configurations:

- Avaya CMS historical data only
- Avaya IC historical data only
- Avaya CMS and Avaya IC historical data

The following table shows the required filegroup or tablespace categories for each configuration.

Filegroups and tablespaces	Avaya CMS only	Avaya IC only	Avaya CMS and Avaya IC
Common OA filegroups or tablespaces	Required	Required	Required
OA with Avaya IC filegroups or tablespaces		Required	Required
OA with CMS filegroups or tablespaces	Required		Required

The only OA requirements are the following:

- There must be at least one datafile per filegroup or tablespace.
- The size of each filegroup or tablespace, including all datafiles, must be at least the minimum size specified on the filegroup or tablespace tables above.
- Depending on your OA configuration, the filegroup or tablespace can get very large. Ask the Avaya PSO personnel to get the output of the OA sizing tool for the maximum size of each database filegroup or tablespace.
- If you choose the size of the filegroup or tablespace to be larger than the single disk capacity and if it has to span on multiple disks, or if you want to have any filegroup or tablespace reside on multiple disks initially, create that filegroup or tablespace manually before you install the OA Historical subsystem. See the database vendor documentation for information on how to create a filegroup or tablespace manually.

Sample historical database layout

No matter which database software you decide to use, you should install the software and assign the filegroups and tablespaces in a logical arrangement. The following table shows an example of how you can arrange the software and filegroups or tablespaces across multiple disks to help improve performance. Consult the Avaya PSO when creating your historical database layout.

Disk ¹	Database		
	SQL	Oracle ²	DB2
1/C	OS software OA software Database software	OS software OA software Database software	OS software OA software Database software (always installed on /usr)
2/E	System log files including: ● Master log ● Msdb log ● Tmpdb log	Oracle SYSTEM tablespace Oracle control file 1	Home directory for DB2 instance USERSPACE1
3/F	SQL Server 2000 data files including: ● Master database datafiles ● Msdb database datafiles ● Tmpdb database datafiles ● HISTADMIN ● HISTIDMAP	Oracle redo log member 1 Oracle USERS tablespace Oracle TOOLS tablespace Oracle control file 2 Oracle archived log files HISTADMIN HISTIDMAP	User temporary tablespace HISTADMIN HISTIDMAP
4/G	Transaction log files including: ● Master database transaction log ● Msdb database transaction log ● Tmpdb database transaction log ● OA database transaction log	Oracle rollback segments tablespace Oracle TEMP tablespace Oracle INDX tablespace Oracle redo log member 2 Oracle control file 3	Transaction log files, including primary logfiles and secondary logfiles
5/H	HISTSTATUS HISTICDISPLAY HISTCMSSYNONYM	HISTSTATUS HISTICDISPLAY HISTCMSSYNONYM	HISTSTATUS HISTICDISPLAY HISTCMSSYNONYM
6/I	HISTICAGENT HISTICAGENTSTATE HISTICAGENTCOMP HISTICAGENTJOB	HISTICAGENT HISTICAGENTSTATE HISTICAGENTCOMP HISTICAGENTJOB	HISTICAGENT HISTICAGENTSTATE HISTICAGENTCOMP HISTICAGENTJOB

Disk ¹	Database		
	SQL	Oracle ²	DB2
7/J	HISTICSVCCCLASS HISTICSVSTATE HISTICJOB HISTICSYSCOMP	HISTICSVCCCLASS HISTICSVSTATE HISTICJOB HISTICSYSCOMP	HISTICSVCCCLASS HISTICSVSTATE HISTICJOB HISTICSYSCOMP
8/K	HISTCMSAGENT HISTCMSCWC	HISTCMSAGENT HISTCMSCWC	HISTCMSAGENT HISTCMSCWC
9/L	HISTCMSVDN HISTCMSSKILL	HISTCMSVDN HISTCMSSKILL	HISTCMSVDN HISTCMSSKILL
10/M	HISTCMSCALLHIST	HISTCMSCALLHIST	HISTCMSCALLHIST

1. A "disk" could also be a partition on one large disk. Filesystems, filegroups, and tablespaces can be split across multiple disks.

2. If the historical database will be larger than 100 GB (the combined used space of all the OA tablespaces), locate the Oracle rollback segments tablespace on one disk by itself and assign the Oracle archive log file destination to a disk by itself, and increase the TEMP tablespace to 5 GB.

The RAM on each machine must meet the minimum requirements shown in [Server machine hardware sizing](#) on page 30. During the growth of the database, be sure that each disk has at least 100 MB free space at all times.

For archive log destinations, you should reserve at least 4 GB of free disk space (assuming you perform the recommended hourly archive backup). Refer to the database documentation for further details.

Installing Microsoft SQL Server 2000 on Windows

This section provides the database options that must be set when installing Microsoft SQL Server 2000 software to support Avaya OA.



Important:

Detailed SQL installation procedures and licensing information are not provided in this section. For detailed information about installation and setup, consult the Microsoft SQL Server 2000 documentation.

This section includes the following topics:

- [Selecting a database configuration](#) on page 60
- [Installing SQL Server 2000 Server and Client tools](#) on page 63
- [Configuring SQL Server 2000](#) on page 64
- [Creating an SQL Server 2000 back-end database](#) on page 65

Selecting a database configuration

Select one of the following configurations to determine which installation procedures must be done:

- [Avaya OA with Avaya IC or CMS, and a back-end database](#) on page 61
- [Avaya OA with Avaya IC or CMS, and a coresident database](#) on page 62

Avaya OA with Avaya IC or CMS, and a back-end database

To create the following configuration:

- Avaya OA, with
- data collection from Avaya IC or CMS, and
- a Microsoft SQL Server 2000 database on a Windows back-end database server machine

do the procedures in the order shown in the following checklist:

Procedure	✓
Verify that the server machine and client machine names are defined properly in the hosts files of all machines. See Appendix B: Networking on page 143.	
Install the SQL Server 2000 Server and Client tools on the back-end database server machine. Follow the procedures in Installing SQL Server 2000 Server and Client tools on page 63.	
If Avaya IC is part of the configuration, install Avaya IC and use Avaya Database Designer to configure databases. Refer to <i>Avaya Interaction Center Release 6.1 Installation and Configuration</i> for more information.	
Configure SQL Server 2000. Follow the guidelines included in Configuring SQL Server 2000 on page 64.	
Create the back-end database. Follow the guidelines included in Creating an SQL Server 2000 back-end database on page 65.	
Install SQL Server 2000 Client tools on the machine where the OA Historical subsystem will be installed. Follow the procedures in Installing SQL Server 2000 Server and Client tools on page 63.	
Configure the OS parameters. Follow the instructions in Making changes on a Windows 2000 server on page 106.	

Avaya OA with Avaya IC or CMS, and a coresident database

To create the following configuration:

- Avaya OA, with
- data collection from Avaya IC or CMS, and
- a Microsoft SQL Server 2000 database on a Windows server machine coresident with the Avaya OA Historical subsystem

do the procedures in the order shown in the following checklist:

Procedure	✓
Verify that the server machine and client machine names are defined properly in the hosts files of all machines. See Appendix B: Networking on page 143.	
Install the SQL Server 2000 Server and Client tools. Follow the procedures in Installing SQL Server 2000 Server and Client tools on page 63.	
If Avaya IC is part of the configuration, install Avaya IC and use Avaya Database Designer to configure databases. Refer to <i>Avaya Interaction Center Release 6.1 Installation and Configuration</i> for more information.	
Configure SQL Server 2000. Follow the guidelines included in Configuring SQL Server 2000 on page 64.	
Configure the OS parameters. Follow the instructions in Making changes on a Windows 2000 server on page 106.	

Installing SQL Server 2000 Server and Client tools

Following the standard installation procedures for the database server software, accept the default options for everything except what is noted below:

Note:

If the installation program does not automatically start, go to the **English/Ent** directory and double-click **autorun.exe**.

- Select **Local Computer**.
- Select **Server and Client Tools** if you are installing a database that will be coresident on the same machine as the Historical subsystem. Select **Client Tools** if you are installing a database on a dedicated (back-end) database server.
- For the instance name, do not use the default name. Select a name and write it down because you will need it when you install the OA Historical subsystem.
- Select a custom software installation, designating where you want the software installed. SQL and OA software can be on the same disk. However, Avaya recommends that data files, including transaction logs, should be placed on a separate disk. See [Sample historical database layout](#) on page 58 for more details.
- When selecting components to install, do not install the **Development Tools** option.
- For the Services Accounts, select **Use the same account for each service** and enter the password for the Administrator login ID. Write down the password because you will need it when you install the OA Historical subsystem. Like all other passwords, keep this information in a safe place.
- For the Authentication Mode, select **Mixed Mode**, and enter and confirm the password for the **sa** login ID.
- For the Collation Settings, select **collation designator**, clear all options under **sort order**, and select the appropriate locale.
- Under **TCP/IP sockets**, enter **1433** for the port number.

Note:

Write down the port number because you will need it when you install the OA Historical subsystem.

- Reboot your system after the installation is finished.

Return to the tables under [Selecting a database configuration](#) on page 60 to determine the next required procedure for your installation.

Configuring SQL Server 2000

The following steps suggest a general configuration for your newly installed database. If your configuration includes Avaya IC, ensure that it is installed and that the Avaya IC tables are created before you configure SQL Server 2000.

To configure SQL and test the installation:

1. Using **Control Panel > Services**, start the **SQLAgent\$instance name** service and set it to run automatically.
2. Limit the amount of memory that the SQL Server can use:
 - a. From the Enterprise Manager, right-click your database instance.
 - b. From the pop-up menu, select **Properties**.
The **SQL Server Properties (Configure)** dialog box is displayed:
 - c. Select the **Memory** tab.
 - d. Select **Dynamically configure SQL Server memory**.
 - e. For **Minimum**, select 25% of the available RAM.
 - f. For **Maximum**, select 50% of the available RAM.
 - g. Select **OK**.
3. Launch the SQL Server Query Analyzer
4. Login using your System Administrator login (**sa**) and password, make sure you select the newly installed SQL server.
5. Make sure you can run some simple queries such as the following:

```
select * from sysdatabases
```

Return to the tables under [Selecting a database configuration](#) on page 60 to determine the next required procedure for your installation.

Creating an SQL Server 2000 back-end database

To create a back-end database for OA:

1. Open the OSQL command line interface.
2. Create the database using the following commands:

```
USE MASTER
GO
CREATE DATABASE BACKEND DATABASE NAME
ON PRIMARY (NAME = BACKEND DATABASE NAMEfile1,
FILENAME = ' DRIVE LOCATION: \mssql\backenddbfile1.mdf ',
SIZE = 1MB,
MAXSIZE = UNLIMITED,
FILEGROWTH = 10%)
LOG ON
(NAME = BACKEND DATABASE NAMELog1,
FILENAME=' DRIVE LOCATION: \mssql\backenddbfile2.ndf ',
SIZE = 5MB,
MAXSIZE = UNLIMITED,
FILEGROWTH = 10%)
GO
```

For example, enter:

```
CREATE DATABASE SampleDatabase
ON PRIMARY (NAME = SampleDatabase_file1,
FILENAME = 'E:\mssql\SampleDatabase_file1.mdf ',
SIZE = 1MB,
MAXSIZE = UNLIMITED,
FILEGROWTH = 10%)
LOG ON
(NAME = SampleDatabase_log1,
FILENAME='E:\mssql\SampleDatabase_log1.ndf ',
SIZE = 5MB,
MAXSIZE = UNLIMITED,
FILEGROWTH = 10%)
GO
```

3. If an error is encountered, drop the database, correct the error, and recreate the database.

Installing the historical database software

4. Add filegroups to the database using the following T_SQL commands from the query analyzer. These commands must be done for all filegroups.

```
ALTER DATABASE BACKEND DATABASE NAME  
ADD Filegroup FILEGROUP NAME
```

For example, enter:

```
ALTER DATABASE SampleDatabase  
ADD Filegroup HistAdmin
```

5. Add datafiles to each of the filegroups using the following commands.

```
ALTER DATABASE BACKEND DATABASE NAME  
ADD FILE  
(NAME = FILEGROUP NAME1,  
FILENAME='E:\mssql\FILEGROUP NAME1.ndf ',  
SIZE = SIZEMB,  
MAXSIZE = UNLIMITED,  
FILEGROWTH = 10%)  
TO FILEGROUP FILEGROUP NAME
```

For example, enter:

```
ALTER DATABASE SampleDatabase  
ADD FILE  
(NAME = HistAdmin_file1,  
FILENAME='E:\mssql\HistAdmin_file1.ndf ',  
SIZE = 400MB,  
MAXSIZE = UNLIMITED,  
FILEGROWTH = 10%)  
TO FILEGROUP HistAdmin
```



CAUTION:

Creating a virtual memory allocation creates a paging file of that size located on the system disk. Ensure that the system disk is created to support this need.

Make sure the virtual memory maximum size for your machine is set to at least as large as physical memory. You must also have enough free disk space in the transaction log destination to accommodate logs generated during the time that a full or incremental backup is running.

6. Space allocations for each of the filegroups should be as indicated by the output of the OA sizing tool available from Avaya PSO personnel.

7. Make the **HistAdmin** filegroup the default filegroup using the following commands:

```
ALTER DATABASE BACKEND DATABASE NAME  
MODIFY FILEGROUP HistAdmin DEFAULT
```

For example, enter:

```
ALTER DATABASE SampleDatabase  
MODIFY FILEGROUP HistAdmin DEFAULT
```

8. Reboot the system.
9. Log in and start the Query Analyzer application to verify that the installation is valid.
10. Return to the tables under [Selecting a database configuration](#) on page 60 to determine the next required procedure for your installation.

Installing Oracle 8i on Windows

This section provides the Oracle database options that must be set when installing Oracle 8i software to support Avaya OA.



Important:

Detailed Oracle installation procedures are not provided in this section. For detailed information about Oracle installation and setup, consult the Oracle 8i documentation.

Topics in this section include:

- [Selecting a database configuration](#) on page 68
- [Installing Oracle 8i database server software on Windows](#) on page 71
- [Configuring an Oracle database instance on Windows](#) on page 71
- [Creating Avaya OA tablespaces on Windows](#) on page 72
- [Installing Oracle 8i database client software on Windows](#) on page 73

Selecting a database configuration

Select one of the following configurations to determine which database options must be set:

- [Avaya OA with Avaya IC or CMS, and a back-end database](#) on page 69
- [Avaya OA with Avaya IC or CMS, and a coresident database](#) on page 70

Avaya OA with Avaya IC or CMS, and a back-end database

To create the following configuration:

- Avaya OA, with
- data collection from Avaya IC or CMS, and
- an Oracle 8i database on a Windows back-end database server machine

do the procedures in the order shown in the following checklist:

Procedure	✓
Verify that the server machine and client machine names are defined properly in the hosts files of all machines. See Appendix B: Networking on page 143.	
Install Oracle on the back-end database server machine. Follow the instructions in Installing Oracle 8i database server software on Windows on page 71.	
Create the initial Oracle database instance on the database server machine. Follow the instructions in Configuring an Oracle database instance on Windows on page 71.	
If Avaya IC is part of the configuration, install Avaya IC and use Avaya Database Designer to configure databases. Refer to <i>Avaya Interaction Center Release 6.1 Installation and Configuration</i> for more information.	
Create the required OA tablespaces on the database server machine. Follow the instructions in Creating Avaya OA tablespaces on Windows on page 72.	
Install the Oracle database client on the machine where the OA Historical subsystem will be installed. Follow the instructions in Installing Oracle 8i database client software on Windows on page 73.	
Configure the OS parameters. Follow the instructions in Making changes on a Windows 2000 server on page 106.	

Avaya OA with Avaya IC or CMS, and a coresident database

To create the following configuration:

- Avaya OA, with
- data collection from Avaya IC or CMS, and
- an Oracle 8i database on a Windows database server machine coresident with the OA Historical subsystem

do the procedures in the order shown in the following checklist:

Procedure	✓
Verify that the server machine and client machine names are defined properly in the hosts files of all machines. See Appendix B: Networking on page 143.	
Install Oracle. Follow the instructions in Installing Oracle 8i database server software on Windows on page 71.	
Create the initial Oracle database instance. Follow the instructions in Configuring an Oracle database instance on Windows on page 71.	
If Avaya IC is part of the configuration, install Avaya IC and use Avaya Database Designer to configure databases. Refer to <i>Avaya Interaction Center Release 6.1 Installation and Configuration</i> for more information.	
Configure the OS parameters. Follow the instructions in Making changes on a Windows 2000 server on page 106.	

Installing Oracle 8i database server software on Windows

Installing the Oracle database software is done for two configurations:

- Coresident on the same machine where the OA Historical subsystem is installed.
- On a back-end database server machine. The OA Historical subsystem is installed on a different server machine in this configuration.

Following the standard installation procedures for the database server software, accept or change the default options for everything except what is noted below:

- Using the custom installation, do not install the Oracle HTTP Server (do not install this option if you are installing the OA Report subsystem on the same server machine; otherwise, you can install this feature)
- During Net8 configuration, note the TCP/IP listen port. The default port is 1521.
- If the database is coresident on the same server where you plan on installing the Historical subsystem, create an Oracle TNS Service Name. This TNS Service Name must be able to connect to the database instance before installing the OA Historical subsystem.

After installing the database server software:

1. Right-click **My Computer** and open **Properties**.
2. Under the **Advanced** tab, select **Environment Variables**.
3. Under **System variables**, find the variable `CLASSPATH`.
4. Append the following to the variable:

`Oracle_location\jdbc\lib\classes12.zip`

5. Click **OK** repeatedly until you are out of the **Properties** dialog boxes.

Return to the tables under [Selecting a database configuration](#) on page 68 to determine the next required procedure for your installation.

Configuring an Oracle database instance on Windows

This section explains which parameters to configure for an Oracle database instance used with the OA Historical subsystem. To determine the size of database your system requires, contact Avaya PSO about using the OA sizing tool.

- Configure at least 115 concurrently dedicated connections.
- Write down the name (instance ID) of your database; this name will be used when you install OA software.
- Set the Character Set and National Character Set to UTF8.

Installing the historical database software

- Set the Rollback segment tablespace size to 4000 MB.
- Set the Temporary tablespace to 2000 MB.
- Set the following Redo Log files to 50 MB.
- For the Logging Parameters, set the Checkpoint Timeout to 0.
- For the SGA Parameters, set the following as shown:
 - Make sure the Shared Pool Size is equal to or larger than 100 MB.
 - Make sure that the Block Buffers is equal to or larger than 300 MB.
 - Make sure that the Block Size is a minimum of 8 MB. Values larger than 8 MB must be in multiples of 8 MB.

Return to the tables under [Selecting a database configuration](#) on page 68 to determine the next required procedure for your installation.

Creating Avaya OA tablespaces on Windows

After you install Avaya IC or Avaya CMS in a configuration with a back-end database server machine, you must manually configure the OA tablespaces on the database server machine.

1. Use Oracle tools to create the tablespaces. Space allocations for each tablespace are determined by the output of the OA sizing tool available from Avaya PSO personnel.
2. If any tablespace will be larger than the maximum size of one disk, add more datafiles to that tablespace.
3. Make sure the virtual memory maximum size for your Windows-based machine is larger than 2 GB.



WARNING:

Creating a virtual memory allocation creates a paging file of the same size on the system disk. Ensure that the system disk is created to support this need. You must also have sufficient free disk space in the archive log destination to accommodate generated logs during the time that a full or incremental backup is running.

4. Return to the tables under [Selecting a database configuration](#) on page 68 to determine the next required procedure for your installation.

Installing Oracle 8i database client software on Windows

The Oracle Database Client software must be installed on the server machine where the OA Historical subsystem will be installed when the historical database server machine is a back-end database server.

Following the standard installation procedures for the database client software, accept or change the default options for everything except what is noted below:

- During Net8 configuration:
 - In the **Net Service Name Configuration, Service Name** dialog box, enter the global database name for the back-end database (for example, `dssdb.oaserver.denver.avaya.com`).
 - In the **Net Service Name Configuration, TCP/IP Protocol** window, enter the host name of the back-end database server machine.
- If you are using a back-end database, create an Oracle TNS Service Name. This TNS Service Name must be able to connect to the database instance before installing the OA Historical subsystem.

After installing the database server software:

1. Right-click **My Computer** and open **Properties**.
2. Under the **Advanced** tab, select **Environment Variables**.
3. Under **System variables**, find the variable `CLASSPATH`.
4. Append the following to the variable:
`Oracle_location\jdbc\lib\classes12.zip`
5. Click **OK** repeatedly until you are out of the **Properties** dialog boxes.

Return to the tables under [Selecting a database configuration](#) on page 68 to determine the next required procedure for your installation.

Installing Oracle 9i on Windows

This section provides the Oracle database options that must be set when installing Oracle 9i software to support Avaya OA.



Important:

Detailed Oracle installation procedures are not provided in this section. For detailed information about Oracle installation and setup, consult the Oracle 9i documentation.

Topics in this section include:

- [Selecting a database configuration](#) on page 74
- [Installing Oracle 9i database server software on Windows](#) on page 77
- [Configuring an Oracle database instance on Windows](#) on page 78
- [Creating Avaya OA tablespaces on Windows](#) on page 78
- [Installing Oracle 9i database client software on Windows](#) on page 79

Selecting a database configuration

Select one of the following configurations to determine which database options must be set:

- [Avaya OA with CMS and a back-end database](#) on page 75
- [Avaya OA with CMS and a coresident database](#) on page 76

Note:

The Oracle 9i database software can only be used for an Avaya OA with Avaya CMS configuration. It cannot be used for an Avaya OA with Avaya IC configuration.

Avaya OA with CMS and a back-end database

To create the following configuration:

- Avaya OA, with
- data collection from CMS only (no Avaya IC), and
- an Oracle 9i database on a Windows back-end database server machine

do the procedures in the order shown in the following checklist:

Procedure	✓
Verify that the server machine and client machine names are defined properly in the hosts files of all machines. See Appendix B: Networking on page 143.	
Install Oracle on the back-end database server machine. Follow the instructions in Installing Oracle 9i database server software on Windows on page 77.	
Create the initial Oracle database instance on the database server machine. Follow the instructions in Configuring an Oracle database instance on Windows on page 78.	
Create the required OA tablespaces on the database server machine. Follow the instructions in Creating Avaya OA tablespaces on Windows on page 78.	
Install the Oracle database client on the machine where the OA Historical subsystem will be installed. Follow the instructions in Installing Oracle 9i database client software on Windows on page 79.	
Configure the OS parameters. Follow the instructions in Making changes on a Windows 2000 server on page 106.	

Avaya OA with CMS and a coresident database

To create the following configuration:

- Avaya OA, with
- data collection from CMS only (no Avaya IC), and
- an Oracle 9i database on a Windows database server machine coresident with the OA Historical subsystem

do the procedures in the order shown in the following checklist:

Procedure	✓
Verify that the server machine and client machine names are defined properly in the hosts files of all machines. See Appendix B: Networking on page 143.	
Install Oracle. Follow the instructions in Installing Oracle 9i database server software on Windows on page 77.	
Create the initial Oracle database instance. Follow the instructions in Configuring an Oracle database instance on Windows on page 78.	
Configure the OS parameters. Follow the instructions in Making changes on a Windows 2000 server on page 106.	

Installing Oracle 9i database server software on Windows

Installing the Oracle database software is done for two configurations:

- Coresident on the same machine where the OA Historical subsystem is installed.
- On a back-end database server machine. The OA Historical subsystem is installed on a different server machine in this configuration.

Following the standard installation procedures for the database server software, accept or change the default options for everything except what is noted below:

- Using the custom installation, do not install Oracle HTTP Server (do not install this option if you are installing the OA Report subsystem on the same server machine; otherwise, you can install this feature)
- During Net8 configuration, note the TCP/IP listen port. The default port is 1521.
- If the database is coresident on the same server where you plan on installing the Historical subsystem, create an Oracle TNS Service Name. This TNS Service Name must be able to connect to the database instance before installing the OA Historical subsystem.

After installing the database server software:

1. Right-click **My Computer** and open **Properties**.
2. Under the **Advanced** tab, select **Environment Variables**.
3. Under **System variables**, find the variable `CLASSPATH`.
4. Append the following to the variable:

`Oracle_location\jdbc\lib\classes12.zip`

5. Click **OK** repeatedly until you are out of the **Properties** dialog boxes.

Return to the tables under [Selecting a database configuration](#) on page 74 to determine the next required procedure for your installation.

Configuring an Oracle database instance on Windows

This section explains which parameters to configure for an Oracle database instance used with the OA Historical subsystem. To determine the size of database your system requires, contact Avaya PSO about using the OA sizing tool.

- Configure at least 115 concurrently dedicated connections.
- Write down the name (instance ID) of your database; this name will be used when you install OA software.
- Set the Character Set and National Character Set to UTF8.
- Set the Rollback segment tablespace size to 4000 MB.
- Set the Temporary tablespace to 2000 MB.
- Set the following Redo Log files to 50 MB.
- For the Logging Parameters, set the Checkpoint Timeout to 0.
- For the SGA Parameters, set the following as shown:
 - Make sure the Shared Pool Size is equal to or larger than 100 MB.
 - Make sure that the Block Buffers is equal to or larger than 300 MB.
 - Make sure that the Block Size is a minimum of 8 MB. Values larger than 8 MB must be in multiples of 8 MB.

Return to the tables under [Selecting a database configuration](#) on page 74 to determine the next required procedure for your installation.

Creating Avaya OA tablespaces on Windows

After you install Avaya CMS in a configuration with a back-end database server machine, you must manually configure the OA tablespaces on the database server machine.

1. Use Oracle tools to create the tablespaces. Space allocations for each tablespace are determined by the output of the OA sizing tool available from Avaya PSO personnel.
2. If any tablespace will be larger than the maximum size of one disk, add more datafiles to that tablespace.
3. Make sure the virtual memory maximum size for your Windows-based machine is larger than 2 GB.

⚠ CAUTION:

Creating a virtual memory allocation creates a paging file of the same size on the system disk. Ensure that the system disk is created to support this need.

You must also have sufficient free disk space in the archive log destination to accommodate generated logs during the time that a full or incremental backup is running.

4. Return to the tables under [Selecting a database configuration](#) on page 74 to determine the next required procedure for your installation.

Installing Oracle 9i database client software on Windows

The Oracle Database Client software must be installed on the server machine where the OA Historical subsystem is to be installed if the historical database server machine will be a back-end database server.

Following the standard installation procedures, accept or change the default options for everything except what is noted below:

- Using the custom installation, do not install Oracle HTTP Server (do not install this option if you are installing the OA Report subsystem on the same server machine; otherwise, you can install this feature)
- During Net8 configuration:
 - In the **Net Service Name Configuration, Service Name** dialog box, enter the global database name for the back-end database (for example, `dssdb.oaserver.denver.avaya.com`).
 - In the **Net Service Name Configuration, TCP/IP Protocol** window, enter the host name of the back-end database server machine.
- If you are using a back-end database, create an Oracle TNS Service Name. This TNS Service Name must be able to connect to the database instance before installing the OA Historical subsystem.

After installing the database server software:

1. Right-click **My Computer** and open **Properties**.
2. Under the **Advanced** tab, select **Environment Variables**.
3. Under **System variables**, find the variable `CLASSPATH`.
4. Append the following to the variable:


```
Oracle_location\jdbc\lib\classes12.zip
```
5. Click **OK** repeatedly until you are out of the **Properties** dialog boxes.

Installing the historical database software

Return to the tables under [Selecting a database configuration](#) on page 74 to determine the next required procedure for your installation.

Installing Oracle 8i on Solaris

This section provides the Oracle database options that must be set when installing Oracle software to support Avaya OA.

**Important:**

Detailed Oracle installation procedures are not provided in this section. For detailed information about Oracle installation and setup, consult the Oracle 8i documentation.

This section includes the following topics:

- [Selecting a database configuration](#) on page 81
- [Installing Oracle 8i database server software on Solaris](#) on page 84
- [Configuring an Oracle database instance on Solaris](#) on page 84
- [Creating Avaya OA tablespaces on Solaris](#) on page 85
- [Installing Oracle 8i database client software on Solaris](#) on page 85

Selecting a database configuration

Select one of the following configurations to determine which installation procedures must be done:

- [Avaya OA with Avaya IC or CMS, and a back-end database](#) on page 82
- [Avaya OA with Avaya IC or CMS, and a coresident database](#) on page 83

Avaya OA with Avaya IC or CMS, and a back-end database

To create the following configuration:

- Avaya OA, with
- data collection from Avaya IC or CMS, and
- an Oracle 8i database on a Solaris back-end database server machine

do the procedures in the order shown in the following checklist:

Procedure	✓
Verify that the server machine and client machine names are defined properly in the hosts files of all machines. See Appendix B: Networking on page 143.	
Install Oracle on the back-end database server machine. Follow the instructions in Installing Oracle 8i database server software on Solaris on page 84.	
Create the initial Oracle database instance on the database server machine. Follow the instructions in Configuring an Oracle database instance on Solaris on page 84.	
If Avaya IC is part of the configuration, install Avaya IC and use Avaya Database Designer to configure databases. Refer to <i>Avaya Interaction Center Release 6.1 Installation and Configuration</i> for more information.	
Create the required OA tablespace on the database server machine. Follow the instructions in Creating Avaya OA tablespaces on Solaris on page 85.	
Install the Oracle database client on the machine where the OA Historical subsystem will be installed. Follow the instructions in Installing Oracle 8i database client software on Solaris on page 85.	
Configure the OS parameters. Follow the instructions in Making changes on a Solaris server on page 108.	

Avaya OA with Avaya IC or CMS, and a coresident database

To create the following configuration:

- Avaya OA, with
- data collection from Avaya IC and CMS (optional), and
- an Oracle 8i database on a Solaris database server machine coresident with the OA Historical subsystem

do the procedures in the order shown in the following checklist:

Procedure	✓
Verify that the server machine and client machine names are defined properly in the hosts files of all machines. See Appendix B: Networking on page 143.	
Install Oracle. Follow the instructions in Installing Oracle 8i database server software on Solaris on page 84.	
Create the initial Oracle database instance. Follow the instructions in Configuring an Oracle database instance on Solaris on page 84.	
Install Avaya IC and use Avaya Database Designer to configure databases. Refer to <i>Avaya Interaction Center Release 6.1 Installation and Configuration</i> for more information.	
Configure the OS parameters. Follow the instructions in Making changes on a Solaris server on page 108.	

Installing Oracle 8i database server software on Solaris

Installing the Oracle database software is done for two configurations:

- Coresident on the same machine where the OA Historical subsystem is installed.
- On a back-end database server machine. The OA Historical subsystem is installed on a different server machine in this configuration.

Following the standard installation procedures, accept or change the default options for everything except what is noted below:

- Using the custom installation, do not install Oracle HTTP Server (do not install this option if you are installing the OA Report subsystem on the same server machine; otherwise, you can install this feature)
- During Net8 configuration, note the TCP/IP listen port. The default port is 1521.
- If the database is coresident on the same server where you plan on installing the Historical subsystem, create an Oracle TNS Service Name. This TNS Service Name must be able to connect to the database instance before installing the OA Historical subsystem.

Return to the tables under [Selecting a database configuration](#) on page 81 to determine the next required procedure for your installation.

Configuring an Oracle database instance on Solaris

This section explains which parameters to configure for an Oracle database instance used with the OA Historical subsystem. To determine the size of database your system requires, contact Avaya PSO about using the OA sizing tool.

- Configure at least 115 concurrently dedicated connections.
- Write down the name (instance ID) of your database; this name will be used when you install OA software.
- Set the Character Set and National Character Set to UTF8.
- Set the Rollback segment tablespace size to 4000 MB.
- Set the Temporary tablespace to 2000 MB.
- Set the following Redo Log files to 50 MB.
- For the Logging Parameters, set the Checkpoint Timeout to 0.
- For the SGA Parameters, set the following as shown:
 - Make sure the Shared Pool Size is equal to or larger than 100 MB.
 - Make sure that the Block Buffers is equal to or larger than 300 MB.

- Make sure that the Block Size is a minimum of 8 MB. Values larger than 8 MB must be in multiples of 8 MB.

- Verify that `remote_login_passwordfile = true`.
- Though not required, Avaya recommends that you change `sort_area_retained_size` to 0.

Return to the tables under [Selecting a database configuration](#) on page 81 to determine the next required procedure for your installation.

Creating Avaya OA tablespaces on Solaris

After you install Avaya IC or Avaya CMS in a configuration with a back-end database server machine, you manually configure the OA tablespaces on the database server machine.

1. Use Oracle tools to create tablespaces as defined by the output of the OA sizing tool available from Avaya PSO personnel.
2. If any tablespace will be larger than the maximum size of one disk, add more datafiles to that tablespace.
3. Return to the tables under [Selecting a database configuration](#) on page 81 to determine the next required procedure for your installation.

Installing Oracle 8i database client software on Solaris

The Oracle client software should be installed on the same machine where the OA Historical subsystem is to be installed when the database server software and database instance will be installed on a back-end database server machine.

Following the standard installation procedures, accept or change the default options for everything except what is noted below:

- During Net8 configuration, note the TCP/IP listen port. The default port is 1521.
- If you are using a back-end database, create an Oracle TNS Service Name. This TNS Service Name must be able to connect to the database instance before installing the OA Historical subsystem.

Return to the tables under [Selecting a database configuration](#) on page 81 to determine the next required procedure for your installation.

Installing Oracle 9i on Solaris

This section provides the Oracle database options that must be set when installing Oracle software to support Avaya OA.



Important:

Detailed Oracle installation procedures are not provided in this section. For detailed information about Oracle installation and setup, consult the Oracle 9i documentation.

This section includes the following topics:

- [Selecting a database configuration](#) on page 86
- [Installing Oracle 9i database server software on Solaris](#) on page 89
- [Configuring an Oracle database instance on Solaris](#) on page 89
- [Creating Avaya OA tablespaces on Solaris](#) on page 90
- [Installing Oracle 9i database client on Solaris](#) on page 90

Selecting a database configuration

Select one of the following configurations to determine which installation procedures must be done:

- [Avaya OA with CMS and a back-end database](#) on page 87
- [Avaya OA with CMS and a coresident database](#) on page 88

Note:

The Oracle 9i database software can only be used for an Avaya OA with Avaya CMS configuration. It cannot be used for an Avaya OA with Avaya IC configuration.

Avaya OA with CMS and a back-end database

To create the following configuration:

- Avaya OA, with
- data collection from CMS only (no Avaya IC), and
- an Oracle 9i database on a Solaris back-end database server machine

do the procedures in the order shown in the following checklist:

Procedure	✓
Verify that the server machine and client machine names are defined properly in the hosts files of all machines. See Appendix B: Networking on page 143.	
Install Oracle on the back-end database server machine. Follow the instructions in Installing Oracle 9i database server software on Solaris on page 89.	
Create the initial Oracle database instance on the database server machine. Follow the instructions in Configuring an Oracle database instance on Solaris on page 89.	
Create the required OA tablespace on the database server machine. Follow the instructions in Creating Avaya OA tablespaces on Solaris on page 90.	
Install the Oracle database client on the machine where the OA Historical subsystem will be installed. Follow the instructions in Installing Oracle 9i database client on Solaris on page 90.	
Configure the OS parameters. Follow the instructions in Making changes on a Solaris server on page 108.	

Avaya OA with CMS and a coresident database

To create the following configuration:

- Avaya OA, with
- data collection from CMS only (no Avaya IC), and
- an Oracle 9i database on a Solaris database server machine coresident with the OA Historical subsystem

do the procedures in the order shown in the following checklist:

Procedure	✓
Verify that the server machine and client machine names are defined properly in the hosts files of all machines. See Appendix B: Networking on page 143.	
Install Oracle. Follow the instructions in Installing Oracle 9i database server software on Solaris on page 89.	
Create the initial Oracle database instance. Follow the instructions in Configuring an Oracle database instance on Solaris on page 89.	
Configure the OS parameters. Follow the instructions in Making changes on a Solaris server on page 108.	

Installing Oracle 9i database server software on Solaris

Installing the Oracle database software is done for two configurations:

- Coresident on the same machine where the OA Historical subsystem is installed.
- On a back-end database server machine. The OA Historical subsystem is installed on a different server machine in this configuration.

Following the standard installation procedures for the database server software, accept or change the default options for everything except what is noted below:

- Using the custom installation, do not install Oracle HTTP Server (do not install this option if you are installing the OA Report subsystem on the same server machine; otherwise, you can install this feature)
- During Net8 configuration, note the TCP/IP listen port. The default port is 1521.
- If the database is coresident on the same server where you plan on installing the Historical subsystem, create an Oracle TNS Service Name. This TNS Service Name must be able to connect to the database instance before installing the OA Historical subsystem.

Return to the tables under [Selecting a database configuration](#) on page 86 to determine the next required procedure for your installation.

Configuring an Oracle database instance on Solaris

This section explains which parameters to configure for an Oracle database instance used with the OA Historical subsystem. To determine the size of database your system requires, contact Avaya PSO about using the OA sizing tool.

- Configure at least 115 concurrently dedicated connections.
- Write down the name (instance ID) of your database; this name will be used when you install OA software.
- Set the Character Set and National Character Set to UTF8.
- Set the Rollback segment tablespace size to 4000 MB.
- Set the Temporary tablespace to 2000 MB.
- Set the following Redo Log files to 50 MB.
- For the Logging Parameters, set the Checkpoint Timeout to 0.
- For the SGA Parameters, set the following as shown:
 - Make sure the Shared Pool Size is equal to or larger than 100 MB.
 - Make sure that the Block Buffers is equal to or larger than 300 MB.

Installing the historical database software

- Make sure that the Block Size is a minimum of 8 MB. Values larger than 8 MB must be in multiples of 8 MB.
- Verify that `remote_login_passwordfile = true`.
- Though not required, Avaya recommends that you change `sort_area_retained_size` to 0.

Return to the tables under [Selecting a database configuration](#) on page 86 to determine the next required procedure for your installation.

Creating Avaya OA tablespaces on Solaris

After you install Avaya IC or Avaya CMS in a configuration with a back-end database server machine, you manually configure the OA tablespaces on the database server machine.

1. Use Oracle tools to create tablespaces as defined by the output of the OA sizing tool available from Avaya PSO personnel.
2. If any tablespace will be larger than the maximum size of one disk, add more datafiles to that tablespace.
3. Return to the tables under [Selecting a database configuration](#) on page 86 to determine the next required procedure for your installation.

Installing Oracle 9i database client on Solaris

The Oracle client software should be installed on the same machine where the OA Historical subsystem is to be installed when the database server software and database instance will be installed on a back-end database server machine.

Following the standard installation procedures for the database client software, accept or change the default options for everything except what is noted below:

- Using the custom installation, do not install Oracle HTTP Server (do not install this option if you are installing the OA Report subsystem on the same server machine; otherwise, you can install this feature)
- During Net8 configuration, note the TCP/IP listen port. The default port is 1521.
- If you are using a back-end database, create an Oracle TNS Service Name. This TNS Service Name must be able to connect to the database instance before installing the OA Historical subsystem.

Return to the tables under [Selecting a database configuration](#) on page 86 to determine the next required procedure for your installation.

Installing DB2 on AIX

This section provides the DB2 database options that must be set when installing DB2 software to support Avaya OA.

**Important:**

Detailed DB2 installation procedures are not provided in this section. For detailed information about DB2 installation and setup, consult the DB2 documentation.

This section includes the following topics:

- [Selecting a database configuration](#) on page 92
- [Installing DB2 software and creating the database instance on AIX](#) on page 94
- [Configuring the database tunables](#) on page 97
- [Manual configuration of Avaya OA tablespaces on DB2](#) on page 99
- [Installing DB2 administration client software on AIX](#) on page 100
- [Troubleshooting the installation](#) on page 103

**Important:**

If your configuration includes Avaya IC, verify that the DB2 installation procedures provided in *Avaya Interaction Center Release 6.1 Installation Planning and Prerequisites* have been followed before you do any additional procedures in this section.

Selecting a database configuration

Select one of the following configurations to determine which installation procedures must be done:

- [Avaya OA with Avaya IC or CMS, and a back-end database](#) on page 92
- [Avaya OA with Avaya IC or CMS, and a coresident database](#) on page 93

Avaya OA with Avaya IC or CMS, and a back-end database

To create the following configuration:

- Avaya OA, with
- data collection from Avaya IC and CMS (optional), and
- a DB2 database on an AIX back-end database server machine

do the procedures in the order shown in the following checklist:

Procedure	✓
Verify that the server machine and client machine names are defined properly in the hosts files of all machines. See Appendix B: Networking on page 143.	
If not already installed, install the DB2 server software and the DB2 administration client software. Follow the instructions in Installing DB2 software and creating the database instance on AIX on page 94.	
If Avaya IC is part of the configuration, install Avaya IC and use Avaya Database Designer to configure databases. Refer to <i>Avaya Interaction Center Release 6.1 Installation and Configuration</i> for more information. Set the tunables using the values shown in Configuring the database tunables on page 97 in addition to any tunables set during IC installation.	
Create the required OA tablespace on the back-end database server machine. Follow the instructions in Manual configuration of Avaya OA tablespaces on DB2 on page 99.	
Install the DB2 administration client on the same machine where the OA Historical subsystem will be installed. Follow the instructions in Installing DB2 administration client software on AIX on page 100.	
Configure the OS parameters. Follow the instructions in Making changes on an AIX server on page 113.	

Avaya OA with Avaya IC or CMS, and a coresident database

To create the following configuration:

- Avaya OA, with
- data collection from Avaya IC and CMS (optional), and
- a DB2 database on an AIX database server machine coresident with the OA Historical subsystem

do the procedures in the order shown in the following checklist:

Procedure	✓
Verify that the server machine and client machine names are defined properly in the hosts files of all machines. See Appendix B: Networking on page 143.	
If not already installed, install the DB2 server software, the DB2 administration client software, and create the database instance on the same machine where the OA Historical subsystem will be installed. Follow the instructions in Installing DB2 software and creating the database instance on AIX on page 94.	
If Avaya IC is part of the configuration, install Avaya IC and use Avaya Database Designer to configure databases. Refer to <i>Avaya Interaction Center Release 6.1 Installation and Configuration</i> for more information. Set the tunables using the values shown in Configuring the database tunables on page 97 in addition to any tunables set during IC installation.	
Configure the OS parameters. Follow the instructions in Making changes on an AIX server on page 113.	

Installing DB2 software and creating the database instance on AIX

Installing the DB2 database software and creating the database instance is done for two configurations:

- Coresident on the same machine where the OA Historical subsystem will be installed.
- On a back-end database server machine. The OA Historical subsystem will be installed on a different server machine in this configuration.



Important:

If your configuration does not include Avaya IC (Avaya CMS and OA standalone configuration), you must do all procedures in this section.

If your configuration includes Avaya IC, verify that the DB2 installation procedures provided in *Avaya Interaction Center Release 6.1 Installation Planning and Prerequisites* have been followed before you do any additional procedures in this section.

This section includes the following topics:

- [Preparing for installation](#) on page 94
- [Installing the database server software](#) on page 95
- [Setting the DB2 registry values and environment](#) on page 96

Preparing for installation

To prepare for DB2 installation:

1. Log in as `root`.
2. Enter the following command to verify that the system has enough space in `/usr`:

```
df -k /usr
```
3. After inserting the DB2 installation CD-ROM, enter:

```
mkdir /cdrom
```

 (if this directory does not already exist)

```
mount -v cdrfs -r /dev/cd0 /cdrom
```
4. Continue with [Installing the database server software](#) on page 95.

Installing the database server software

Following the standard installation procedures for the database server software, accept the default options for everything except what is noted below:

- Use the `/cdrom/db2setup` command to start the installation. If you use any other tools to set up the database, you must do several procedures manually. The standard `db2setup` command will do all procedures automatically.
- Select the following products:
 - DB2 Administration Client
 - DB2 UDB Enterprise Edition
- Customize the DB2 Administration Client selecting the following components:
 - Java Support
 - Control Center
- Customize the DB2 UDB Enterprise Edition selecting the following components:
 - Java Support
 - Control Center
- Customize the DB2 UDB Enterprise Edition clearing the following components:
 - Replication
- Click **OK** for all conditions and queries.
- In the **Create DB2 Services** dialog box, select the following items:
 - Create a DB2 instance
 - Create the Administration Server
- Customize the Administration Server, if needed. The following is an example using the default settings:
 - User Name - enter `db2as`
 - User ID - allow the system to assign a default ID
 - Group Name - enter `db2asgrp`
 - Group ID - allow the system to assign a default ID
 - Home Directory - enter `/home/db2as`
 - Password and Verify Password - enter and confirm the password for the user ID
- Customize the DB2 Instance, setting the following options:
 - User Name - enter `db2inst1`
 - User ID - allow the system to assign a default ID
 - Group Name - enter `db2iadm1`

Installing the historical database software

- Group ID - allow the system to assign a default ID
- Home Directory - enter an installation location different from the default disk, if possible. See [Sample historical database layout](#) on page 58 for a suggested layout.
- Password and Verify Password - enter and confirm the password for the user ID



Important:

Avaya recommends that you use the default database instance settings. If you use a different setting, note those settings as they are used later when OA is installed.

Continue with [Setting the DB2 registry values and environment](#) on page 96

Setting the DB2 registry values and environment

To set the registry values and set other environment variables:

1. Use the following commands to set the DB2 registry values and environment:

```
. ~INSTANCE_ID/.profile
```

```
db2set DB2_INDEX_2BYTEVARLEN=yes
```

```
db2set DB2_RR_TO_RS=YES_OVERRIDE_RI (required only for an IC configuration)
```

```
db2set DB2_STRIPED_CONTAINERS=yes (required only for an IC configuration)
```

```
db2set DB2ENVLIST=EXTSHM (required only for an IC configuration)
```

```
db2set DB2COMM=tcpip
```

```
db2set DB2AUTOSTART=TRUE
```

where *INSTANCE_ID* is the DB2 database instance name (default is `db2inst1`).

2. If you are using a different user ID than the default `db2inst1` instance owner to manage and access the database (for example, `biadmin` to create, manage, and access the database), make sure you add that user to the `SYSADM` group. For example, to add `db2iadm1`, use:

```
db2 get dbm config | grep SYSADM_GROUP
```

to obtain the name of the `SYSADM` group. If you are using `root` to create the initial database, then `root` must also be in `SYSADM_GROUP`. Use the command `smitty` to add `root` to the group.

3. Install all recommended DB2 fix packs. See [Software required for the historical database and Historical subsystem servers](#) on page 34 for the latest DB2 fix packs.
4. Return to the tables under [Selecting a database configuration](#) on page 92 to determine the next required procedure for your installation.

Configuring the database tunables

Consider configuring the database tunables and data manager tunables shown in this section to optimize OA and DB2 interactions. Consult *IBM DB2 Administration Guide: Performance* for detailed information.

Database tunable	Description
applheapsz	Increase to accommodate aggregation queries and Cognos cube generation.
avg_appls	Increase to improve DB efficiency for multiple applications.
locklist	Improves OA process concurrency. Increase to avoid escalations to table locks.
logbufsiz	Increase to accommodate large transactions and minimize I/O.
logfilesize logprimary logsecondary	Increase to accommodate database transactions. Balance logfilesize and number of logfiles.
log_retain	Administer according to database recovery strategy.
maxlocks	Improves OA process concurrency. Increase to avoid escalations to table locks.
newlogpath	Administer location of logfiles.
num_io_cleaners	Increase to reduce wait time for buffer reads.
num_io_servers	Increase to maximize pre-fetch I/O.
sortheap	Increase to accommodate aggregation and Advanced Reporting cube creation queries.
stat_heap_size	Increase if statistics take too long, or when using the <code>runstats</code> command with distribution.
stmtheap	Increase SQL statement heap to accommodate complex and large queries.
stmt_heap_size	Increase to accommodate large queries.
user_exit	Administer according to database recovery strategy.

Installing the historical database software

Database manager tunable	Description
maxagents	Increase to accommodate concurrent database access. Critical in common IC/OA environment. Avaya recommends that you set this to 500.
maxappls	Avaya recommends that you set this to 500.
num_initagents num_poolagents	Increase to avoid startup cost of agents.
query_heap_sz	Increase to provide additional memory to accommodate aggregation.
sheapthres	Increase to provide additional sort memory for concurrent applications. Ideally, this should be 500 times the value of the sortheap database tunable. At a minimum, set this to 100 times the sortheap tunable.

If you change any of the tunables, enter the following commands to stop and restart the database:



Important:

The database and instance may need to be restarted every time you change any of the tunables.

db2stop force (this terminates all connections to the database)

db2start

Return to the tables under [Selecting a database configuration](#) on page 92 to determine the next required procedure for your installation.

Manual configuration of Avaya OA tablespaces on DB2

You must manually configure the OA tablespaces on the database server machine for the following configurations:

- When reusing an existing database and tablespaces.
- When you are using Avaya IC or Avaya CMS in a configuration with a back-end (dedicated) database server machine.

Optionally, you may manually configure the OA tablespaces on the database server machine if you have an OA and Avaya CMS standalone configuration. If you do not manually configure the tablespaces, OA will do it automatically for you.

To manually configure the tablespaces:

1. Use DB2 tools to create tablespaces as defined by the output of the OA sizing tool available from Avaya PSO personnel.

The following is an example of how you would create a buffer pool called **OABUFFER** and associate the tablespaces to **OABUFFER**:

```
db2 "CONNECT TO DATABASE_ALIAS"
db2 "CREATE BUFFERPOOL OABUFFER SIZE 10000 PAGESIZE 8 K EXTENDED STORAGE"
db2 "DISCONNECT ALL"
db2 "RESTART DATABASE DATABASE_ALIAS"
db2 "CONNECT TO DATABASE_ALIAS"
db2 "CREATE REGULAR TABLESPACE TABLESPACE_NAME PAGESIZE 8 K MANAGED BY
DATABASE USING (FILE '/DIRECTORY_NAME/TABLESPACE_NAME' 51200) EXTENTSIZE 16
OVERHEAD 11.67 PREFETCHSIZE 16 TRANSFERRATE 0.31 BUFFERPOOL OABUFFER"
```

where **DATABASE_ALIAS** is the name of the database alias, **TABLESPACE_NAME** is the name of the tablespace, and **DIRECTORY_NAME** is the location of the tablespace.

2. If any tablespace will be larger than the maximum size of one disk, add more datafiles to that tablespace.
3. Return to the tables under [Selecting a database configuration](#) on page 92 to determine the next required procedure for your installation.

Installing DB2 administration client software on AIX

When the DB2 server software and database instance is installed on a back-end (dedicated) database server machine, the DB2 administration client software must be installed on the same machine where the OA Historical subsystem will be installed.

This section includes the following topics:

- [Setting up the OS](#) on page 100
- [Installing the DB2 administration client software and setting the database alias](#) on page 101

Setting up the OS

To set up the OS for the DB2 installation:

1. Log in as `root`.
2. Enter the following commands to verify that the system has enough space on `/opt` or `/usr`:

```
df -k /opt
```

```
df -k /usr
```
3. After inserting the DB2 installation CD-ROM, enter:

```
mkdir /cdrom
```

 (if this directory does not already exist)

```
mount -v cdrfs -r /dev/cd0 /cdrom
```
4. Continue with [Installing the DB2 administration client software and setting the database alias](#) on page 101.

Installing the DB2 administration client software and setting the database alias

Following the standard installation procedures for the DB2 administration client software, accept the default options for everything except what is noted below:

- Use the `/cdrom/db2setup` command to start the installation. If you use any other tools to set up the database, you must do several procedures manually. The standard `db2setup` command will do all procedures automatically.
- Select the following products:
 - DB2 Administration Client
- Customize the DB2 Administration Client selecting the following components:
 - Java Support
 - Control Center
- Create a DB2 instance
- Create the Administration Server



Important:

Avaya recommends that you use the default database instance settings. If you use a different setting, note those settings as they are used later when OA is installed.

- Create a database alias to the historical database using the following procedure:

Note:

In this procedure:

- *INSTANCE_ID* matches the ID used when the DB2 database instance was installed (the default instance ID is `db2inst1`)
- *INSTANCE_ID_HOME* is the home directory of the database instance ID (for example, `/home/db2inst1`)
- *SERVER_NAME* is the name of the server where the database is installed
- *PORT_NUMBER* is the port number used by `db2cINSTANCE_ID` (you can find this value in `/etc/services` on the database server)
- *REAL_DATABASE_NAME* is the name of the OA database
- *PASSWORD* is the password for the database instance ID

1. Enter:

```
. $INSTANCE_ID_HOME/.profile
```

Installing the historical database software

2. Enter commands similar to the following to create the alias (these commands are an example):

```
db2 "FORCE APPLICATIONS ALL"

db2 "catalog tcpip node OA_NODE remote SERVER_NAME server
    PORT_NUMBER"

db2 "catalog db REAL_DATABASE_NAME as OADB_AKA at node OA_NODE"

db2 "terminate"

db2start

db2 "attach to OA_NODE user INSTANCE_ID using PASSWORD" (this is an
optional step to make the OA_NODE the default node)
```

3. List the node and the database, for example:

```
db2 "list db directory"

db2 "list node directory"
```

4. Test the connection, for example:

```
db2 "connect to OADB_AKA user INSTANCE_ID using PASSWORD"

db2 "set schema OASchema"

db2 "select * from subsystem"
```



Important:

When installing OA, verify that you assign the database alias name in the **OA Database Name** field to connect to the back-end database.

5. Install all recommended DB2 fix packs. See [Software required for the historical database and Historical subsystem servers](#) on page 34 for the latest DB2 fix packs.

Return to the tables under [Selecting a database configuration](#) on page 92 to determine the next required procedure for your installation.

Troubleshooting the installation

While installing the DB2 software, you can use the following command to verify the installation:

```
lsldpp -la | grep "db2*"
```

Each of the components should display the format 7.1.0.XX.

To verify that the software was installed and the database instance was created:

1. Enter the following command to create a sample database:

```
db2 "create database sample"
```

2. Enter the following command to start the DB2 Control Center:

```
db2cc
```

You should see your sample database. For non-english language systems you might have to do an export of the LANG env variable (for example, "**export LANG=zh_CN**") in order to see Chinese characters.

If the software fails to install, check `/tmp/db2setup.log`. Possible failures include permission problems, the software is already installed, or directories already exist from a previous install.

If there is a problem with the Administration server, remove `/home/db2as/sql1lib` and run the following command:

```
/usr/lpp/db2_07_01/instance/dasicrt db2as
```

Redo `db2setup`, if needed, using the procedure for creating a DB2 instance.

If the database instance could not be created or services could not be started, check `/tmp/db2setup.log`. Possible failures include permission problems or that the instance owner home directory does not exist (for example, `/home/db2inst1`). Correct the problem and run the following command:

```
/usr/lpp/db2_07_01/instance/db2icrt -a SERVER -u db2fenc1  
db2inst1
```

Installing the historical database software

■ ■ ■ ■ ■ ■

Creating users and setting OS parameters

You must create user IDs, group IDs, and set certain OS parameters before Avaya OA software is installed on the server machines. You only have to set these OS parameters on machines where the historical database software and the OA software are installed.

This section includes the following topics:

- [Making changes on a Windows 2000 server](#) on page 106
- [Making changes on a Solaris server](#) on page 108
- [Making changes on an AIX server](#) on page 113

Making changes on a Windows 2000 server

When installing OA on a server machine that is using Windows 2000, you must do the procedures noted in the following sections:

- [Creating user IDs and group IDs on Windows servers](#) on page 106
- [Configuring Real-time subsystem locale settings on Windows](#) on page 107

Creating user IDs and group IDs on Windows servers

Before you can begin OA installation, you must create user IDs and group IDs on servers where the OA software will be installed. User IDs can be added to or removed from group IDs using the operating system management tools. After you create user IDs, you must have the owners of the user IDs change the default password before OA is installed.



Important:

The user ID and group ID values created here *must* be used when setting user and group ID options during OA installation. Note these values and provide them to the person installing OA.

Create the following group IDs for the Administration client and Report client:

- For the Administration client software, **oaadmin** (default, recommended name). The administration group is used to identify users who can use the Administration client. This group ID must be created on every server machine where OA software will be installed.
- For the Report client software, **oarpt** (default, recommended name). The report group is used to identify members who can use the OA reports. This group ID must be created on the server where the Historical subsystem is to be installed.

Create the following IDs on all server machines where OA software will be installed:

- group ID = **oaadmin**
- user ID = **biadmin**

These IDs are used while you are installing Avaya OA.

Configuring Real-time subsystem locale settings on Windows

For Windows installations that use localized reports, you must set the Windows regional options so that the reports display the proper language. If the regional settings are not correct, the reports will, by default, display in U.S. English.

To configure the locale settings:

1. Select **Start > Settings > Control Panel**.
2. Select **Regional Options**.
3. Select the **General** tab.
4. Select the locale for your system using the locales available in the **Your locale** drop-down box. Use the locale settings shown in the following table:

Desired language	Your locale setting
Chinese	Chinese (PRC)
English	English (United States)
French	French (France)
German	German (Germany)
Italian	Italian (Italy)
Japanese	Japanese
Korean	Korean
Portuguese	Portuguese (Brazil)
Spanish	Spanish (Colombia)
Thai	Thai

If you cannot find your language in the drop-down list, add the required language sets using **Language settings for the system**.

Making changes on a Solaris server

When installing OA on a server machine that is using Solaris, you must do the procedures noted in the following sections:

- [Creating user IDs and group IDs on Solaris servers](#) on page 108
- [Configuring locale settings in Solaris](#) on page 110
- [Configuring Real-time subsystem parameters](#) on page 111

Creating user IDs and group IDs on Solaris servers

Before you can begin OA installation, you must create user IDs and group IDs on servers where the OA software will be installed. User IDs can be added to or removed from group IDs using the operating system management tools. After you create user IDs, you must have the owners of the user IDs change the default password before OA is installed.



Important:

The user ID and group ID values created here *must* be used when setting user and group ID options during OA installation. Note these values and provide them to the person installing OA.

Although possible, it is *not* recommended that you use the `root` user ID for this account. Using this superuser ID would create a security risk because all of the OA processes and jobs would run as a privileged user and have access to the whole system. The user ID must be created on the host before installing OA.

Create the following group IDs for the Administration client and Report client:

- For the Administration client software, `oaadmin` (default, recommended name). The administration group is used to identify users who can use the Administration client. This group ID must be created on every server machine where OA software will be installed.
- For the Report client software, `oarpt` (default, recommended name). The report group is used to identify members who can use the OA reports. This group ID must be created on the server where the Historical subsystem is to be installed.

Create the following IDs on all server machines (including CMS server machines) where OA software will be installed:

- group ID = `oaadmin`
- user ID = `biadmin`

These IDs are used while you are installing Avaya OA.



Important:

When administering these groups, the group ID *must* be the primary group ID for the user ID. This is required during installation of OA software.

On a Solaris server machine, use the `groupadd` and `useradd` command-line commands to create these IDs. You can also use the **Admintool**, which is a GUI-based tool. To access **Admintool**, right-click on the desktop, select **Applications > Application Manager**, select **System_Admin**, and select **Admintool**.

On a Solaris server machine, the user ID can be administered via NIS. If you add a non-NIS user ID, the location of the home directory for the user ID is, by default, `/export/home`. If you add an NIS user ID, you must provide a non-system directory for the installation path to the user ID.

On a CMS R3V11 Solaris server machine, the `biadmin` user ID must be added to the password aging exclude file located at `/cms/db/age_pw_exclude`.

On a CMS Solaris server machine, the `informix` user ID must have a password assigned because this user ID is required during installation of OA software.

Configuring locale settings in Solaris

Before OA is installed, you must configure the `LANG` variable on Solaris systems where you will be installing localized software.

To configure the locale settings:

- 1. Log in as `root`.
- 2. Enter:

```
vi /etc/default/init
```
- 3. Add one or more lines to the file that defines the language software that will be installed. The line is formatted as:

`LANG=language`

where *language* is one of the following:

Language	Value
Chinese (simplified)	zh_CN.UTF-8
English (U.S.)	en_US.UTF-8
French (France)	fr_FR.UTF-8
German (traditional)	de_DE.UTF-8
Italian	it_IT.UTF-8
Japanese	ja_JP.UTF-8
Korean	ko_KR.UTF-8
Portuguese (Brazilian)	pt_BR.UTF-8
Spanish (Colombian)	es_CO.UTF-8
Thai	th_TH.UTF-8

- 4. Press **Esc**.
- 5. Enter:

`:wq!`

This writes and quits the file.

Configuring Real-time subsystem parameters

The following configuration procedures must be done when you are installing the TimesTen Real-time subsystem on a Solaris server machine:

- [Configuring semaphores](#) on page 111
- [Configuring message logging](#) on page 112

Configuring semaphores

The number of semaphores you configure are in addition to the values previously administered for a standard Solaris installation. For example, if the semaphore `seminfo_semmns` parameter is already set to 310, you must set the value to 2310 to support the TimesTen database.

To configure the semaphores on Solaris:

1. Log in to the Solaris server machine as `root`.
2. Enter:

`vi /etc/system`
3. Edit the following lines in `/etc/system` to set the value. If the kernel setting does not exist in the file, add a new line to the `/etc/system` file.

Kernel settings	Increase by...
<code>set semsys:seminfo_semmni</code>	20
<code>set semsys:seminfo_semmsl</code>	100
<code>set semsys:seminfo_semmns</code>	2000
<code>set semsys:seminfo_semmnu</code>	2000
<code>set shmsys:shminfo_shmmax</code>	Set to the amount of RAM installed on the server machine (if not already configured)

4. Press **Esc**.
5. Enter:

`:wq!`
This writes and quits the file.
6. Enter:

`/usr/sbin/shutdown -y -i6 -g0`
This reboots the machine.

Configuring message logging

TimesTen generates error, warning, informational, and debug messages to assist in troubleshooting.



CAUTION:

The path used for the setup of the log files must match the path used when installing the Real-time subsystem, in this case `/export/home/biadmin`. If you use a different path here, you must use the same path in [Installing Avaya OA components on a Solaris platform](#) on page 46 in *Avaya Operational Analyst Release 6.1 Installation and Configuration*.

To configure the system to save these messages in a directory:

1. Log in to the Solaris server machine as `root`.

2. Enter:

```
vi /etc/syslog.conf
```

3. Add the following line to the end of the file:

```
user.info      /export/home/biadmin/TimesTen4.5/32/logs/tt.log
```

When entering the line, enter a Tab between `user.info` and `/export`.

4. Press **Esc**.

5. Enter:

```
:wq!
```

This writes and quits the file.

6. Enter the following commands to create the log file directory:

```
cd /export/home/biadmin/TimesTen4.5/32
```

```
mkdir logs
```

7. Enter:

```
vi tt.log
```

8. Press **Return** to create a blank line.

9. Press **Esc**.

10. Enter:

```
:wq!
```

This writes and quits the file.

11. Restart the `syslogd` daemon so that the changes take effect.

Making changes on an AIX server

When installing OA on a server machine that is using AIX, you must do the procedures noted in the following sections:

- [Creating user IDs and group IDs on AIX servers](#) on page 113
- [Configuring message logging](#) on page 114

Creating user IDs and group IDs on AIX servers

Before you can begin OA installation, you must create user IDs and group IDs on servers where the OA software will be installed. User IDs can be added to or removed from group IDs using the operating system management tools. After you create user IDs, you must have the owners of the user IDs change the default password before OA is installed.



Important:

The user ID and group ID values created here *must* be used when setting user and group ID options during OA installation. Note these values and provide them to the person installing OA.

Although possible, it is not recommended that you use the `root` user ID for this account. Using these superuser IDs would create a security risk because all of the OA processes and jobs would run as a privileged user and have access to the whole system. The user ID must be created on the host before installing OA.

Create the following group IDs for the Administration client and Report client:

- For the Administration client software, `oaadmin` (default, recommended name). The administration group is used to identify users who can use the Administration client. This group ID must be created on every server machine where OA software will be installed.
- For the Report client software, `oarpt` (default, recommended name). The report group is used to identify members who can use the OA reports. This group ID must be created on the server where the Historical subsystem is to be installed.

Create the following IDs on all server machines where OA software will be installed:

- group ID = `oaadmin`
- user ID = `biadmin`

These IDs are used while you are installing Avaya OA.



Important:

When administering these groups, the group ID *must* be the primary group ID for the user ID. This is required during installation of OA software.

On an AIX server machine, use the `groupadd`, `smit`, `smitty`, or `wsm` commands to create these IDs.

On an AIX server machine, the user ID can be administered via NIS. If you add a non-NIS user ID, the location of the home directory for the user ID is, by default, `/home`. If you add an NIS user ID, you must provide a non-system directory for the installation path to the user ID.

Configuring message logging

TimesTen generates error, warning, informational, and debug messages to assist in troubleshooting.



CAUTION:

The path used for the setup of the log files must match the path used when installing the Real-time subsystem, in this case `/home/biadmin`. If you use a different path here, you must use the same path in [Installing Avaya OA components on an AIX platform](#) on page 64 in *Avaya Operational Analyst Release 6.1 Installation and Configuration*.

To configure the system to save these messages in a directory:

1. Log in to the AIX server machine as `root`.

2. Enter:

```
vi /etc/syslog.conf
```

3. Add the following line to the end of the file:

```
user.info      /home/biadmin/TimesTen4.5/32/logs/tt.log    rotate size 100k files 3
```

When entering the line, enter a Tab between `user.info` and `/home` and between `tt.log` and `rotate`. The `rotate` keyword specifies that the logfiles will be rotated based on the `size` (100k in this example) and the number of `files` (3 in this example).

4. Press **Esc**.

5. Enter:

```
:wq!
```

This writes and quits the file.

6. Enter the following commands to create the log file directory:

```
cd /home/biadmin/TimesTen4.5/32
mkdir logs
```

7. Enter:

```
vi tt.log
```

8. Press **Return** to create a blank line.

9. Press **Esc**.

10. Enter:

```
:wq!
```

This writes and quits the file.

11. Restart the `syslogd` daemon so that the changes take effect.

■ ■ ■ ■ ■ ■

Setting up Web servers

This section describes how to install Web server software on machines where the OA Report subsystem software is also installed. Every machine where the OA Report subsystem is installed must also have Web server software installed.

This section includes the following topics:

- [Installing the IIS Web server on Windows](#) on page 118
- [Installing and configuring Sun ONE Web Server on a Solaris machine](#) on page 119
- [Installing and configuring WebSphere on an AIX machine](#) on page 121

Installing the IIS Web server on Windows

For Windows, the IIS Web server software is normally installed as part of the prerequisite software installation described in [Server software requirements](#) on page 33. However, there are conditions when the normal installation of the IIS software must be altered (see [Report server considerations](#) on page 25).

Do one of the following:

- If you know that you will need to alter your IIS software installation:

1. Record the security settings of your existing Web server:



Important:

Record these settings before you install the OA Report subsystem.

- a. Select **Start > Programs > Administrative Tools > Internet Services Manager**.
 - b. Expand the tree view: **server-name > Default Web Site** and right click on **Default Web Site > Properties**
 - c. Select the **Directory Security** tab.
 - d. Click on the **Edit** button under the Anonymous access and authentication control section.
 - e. If **Anonymous access** is selected, click the **Edit** button next to **Account used for anonymous access** and record the information in the resulting window for later use.
2. Install the OA Report subsystem on the same Windows server as described in [Preparing for installation](#) on page 11 and [Installing Avaya OA components on a Windows platform](#) on page 28 in *Avaya Operational Analyst Release 6.1 Installation and Configuration*.
 3. Alter the IIS installation as described in [Configuring IIS on Windows for coresident Avaya IC and Avaya OA](#) on page 101 of *Avaya Operational Analyst Release 6.1 Installation and Configuration*.
- If no alterations are required for the Web server installation:
 1. If your configuration includes Avaya IC, confirm that Avaya IC has been installed and configured as described in *Avaya Interaction Center Release 6.1 Installation and Configuration*.
 2. Install OA as described in [Preparing for installation](#) on page 11 in *Avaya Operational Analyst Release 6.1 Installation and Configuration*.

Installing and configuring Sun ONE Web Server on a Solaris machine

To install and set up the Sun ONE Web Server software:

1. Log in as `root`.
2. If you have not already purchased the software, you can download it from Sun at:
http://www.sun.com/software/products/web_srvr/home_web_srvr.html

The supported software version is shown in [Software required for Report servers](#) on page 38.

3. Move (`cd`) to the directory where you copied or downloaded the installation files.
4. Enter:

```
./setup
```

The installation script starts and the welcome screen is displayed.

5. Press **Enter**.

The license agreement screen is displayed.

6. Enter:

```
yes
```

7. Press **Enter**.

The installation type screen is displayed.

8. Select **Typical installation** and press **Enter**.

9. The installation script then begins a series of questions to set the installation options.
Set the options as shown in the following table:

Installation option	Setting
Install location	Enter <code>/usr/iplanet/servers</code>
Web server components to install	Press Enter to select all
Components to install [1,2,3,4,5]	Press Enter to select all
Domain name	Enter the fully-qualified domain name for the Web server; for example, <code>oadenver.denver.avaya.com</code>

Setting up Web servers

Installation option	Setting
Note: Avaya recommends that the System user and System group options be set to the user ID and group ID used when installing OA. See Creating user IDs and group IDs on Solaris servers on page 108.	
System user	<code>biadmin</code> (default)
System group	<code>oaadmin</code> (default)
Run iWS Administration Server as [root]	Enter <code>root</code> if you want to start the Web service from the admin console; otherwise, use a user ID of your choice as described in the installation script notes
iWS Administration Server User Name	Enter <code>admin</code>
iWS Administration Server Password	Enter and confirm a password for the <code>admin</code> user ID
iWS Administration Server Port	<code>8888</code>
Web Server Port	Enter a port number in the range of 1024 to 65535; 7000 is recommended unless already in use
Web Server Content Root	Press Enter to accept default
Install Sun version of JRE and JDK	Enter <code>no</code> to install the default components; do not install different versions

10. After all the options have been set, press **Enter** to begin the installation.
11. When the installation is finished, you are given instructions for running the Web server software. Skip those instructions at this time.
12. If your configuration includes Avaya IC, install and configure Avaya IC as described in *Avaya Interaction Center Release 6.1 Installation and Configuration*.
13. Install OA by continuing with [Preparing for installation](#) on page 11 in *Avaya Operational Analyst Release 6.1 Installation and Configuration*.

Installing and configuring WebSphere on an AIX machine

The procedures in this section describe how to install and configure the WebSphere software on an AIX server.

This section includes the following topics:

- [Prerequisites](#) on page 121
- [Path definitions](#) on page 122
- [Installing WebSphere](#) on page 122
- [Changing the administration port](#) on page 122
- [Configuring the server](#) on page 124

Prerequisites

Before installing WebSphere:

- Check to see if the HTTP Server software is installed on the machine. If it is installed and the version is older than 1.3.26.1, uninstall the HTTP Server software from the machine.
- Verify that there is at least 512 MB of free space in `/usr`, which is the default installation location, before you install WebSphere.
- Confirm which user ID you will use when installing OA (for example, `biadmin` user ID and `oaadmin` group ID). See [Creating user IDs and group IDs on AIX servers](#) on page 113 for more information.
- Determine if you want to "secure" the login of the WebSphere Administrative Console. Avaya recommends that the customer create a secure user ID. If this is desired, select a user ID and password and administer this in the OS.
- Determine if the IC Web Channel and the OA Report subsystem will be installed on the same server machine. If they will be installed on the same machine, there must be two instances of the HTTP Server software installed on that machine. You must determine:
 - where the HTTP Server software was installed for Avaya IC, typically in the default location, `/usr/IBMHttpServer/bin`, and
 - where the HTTP Server software will be installed for OA, typically in a nonstandard location, for example, `/usr/OA_IBMHttpServer/bin`.

Path definitions

In this section, the variable `$WEBSphere_HOME` represents the installation path for WebSphere. The default installation path is `/usr/WebSphere/AppServer`.

Installing WebSphere

Following the standard installation procedures for WebSphere:

1. Log in as `root`.
2. Select a custom installation.
3. Select the **IBM HTTP Server** option.
4. Clear the **Embedded Messaging**, **Application Server Samples**, and **J2EE** options unless the customer requires these options. If the machine is being used only for OA, these options are not needed.
5. If the IC Web Channel and the OA Report subsystem will be installed on the same server machine, there must be two instances of the HTTP Server software installed on that machine. You must determine where the HTTP Server software was installed for Avaya IC, which is typically in the default location `/usr/IBMHttpServer/bin`. Once that location has been determined, you must select a different location where the HTTP Server software will be installed for OA, for example, `/usr/OA_IBMHttpServer/bin`.
6. Accept all other defaults.

Changing the administration port

You must change the administration port if it is currently set to the default value of 9090.

To check the current value of the administration port and change it if needed:

1. Enter:

```
grep 9090 /etc/services
```

If a line similar to the following is displayed, continue with Step 2. If a line is not displayed, you may skip this procedure.

wsmserver	9090/tcp
-----------	----------

2. Enter:

```
cd $WEBSPPHERE_HOME/config/cells/hostname/nodes/hostname/
servers/server1
```

where *hostname* is the name of the server where you installed WebSphere.

3. Enter:

```
vi server.xml
```

4. Search for port number 9090 and change it to an unused port number, for example, 9095. The port selected cannot conflict with any ports used by Avaya IC or other OA applications.

5. Press **Esc**.

6. Enter:

```
:wq!
```

This writes and quits the file.

7. Enter:

```
cd $WEBSPPHERE_HOME/config/cells/hostname
```

where *hostname* is the name of the server where you installed WebSphere.

8. Enter:

```
vi virtualhosts.xml
```

9. Search for port number 9090 and change it to the same port number, for example, 9095. The port selected cannot conflict with any ports used by Avaya IC or other OA applications.

10. Press **Esc**.

11. Enter:

```
:wq!
```

This writes and quits the file.

Configuring the server

There are several procedures you must do to configure the server:

- [Starting WebSphere and the Administrative Console](#) on page 124
- [Administering WebSphere to run as a non-root user](#) on page 125
- [Configuring resource settings](#) on page 125
- [Removing the default application](#) on page 126
- [Changing file permissions](#) on page 127
- [Starting WebSphere](#) on page 127
- [Changing the HTTP Server properties \(optional\)](#) on page 128
- [Creating a secure login by enabling Global Security \(optional\)](#) on page 129

Starting WebSphere and the Administrative Console

To start WebSphere and the Administrative Console:

1. Enter:

```
. ~INSTANCE_ID/.profile  
cd $WEBSphere_HOME/bin  
./startServer.sh -user userID -password userpassword server1
```

where:

- *INSTANCE_ID* matches the ID used when the DB2 database instance was installed. The default instance ID is `db2inst1`.
- *userID* is the user ID administered for Global Security on WebSphere, if administered.
- *userpassword* is the password for that user ID, if administered.

2. Using a browser window, enter:

```
http://machinename:portnumber/admin
```

where *machinename* is the server machine name where WebSphere is installed and *portnumber* is the new administration port number from [Changing the administration port](#) on page 122.

3. Log in with an administrator user ID.

Administering WebSphere to run as a non-root user

To administer WebSphere to run as non-root user:

1. In the left frame of the Administrative Console, select **Servers > Application Servers**.
2. In the main frame, select **server1**.
3. Scroll down and select **Process Definition**.
4. Scroll down and select **Process Execution**.
5. In the **Run As User** field, enter the user ID you plan to use to install OA (for example, **biadmin**). This user ID will be entered later in OA installation and must match. See [Creating user IDs and group IDs on AIX servers](#) on page 113 for more information.
6. In the **Run As Group** field, enter the group ID you plan to use to install OA (for example, **oaadmin**). This group ID will be entered later in OA installation and must match. See [Creating user IDs and group IDs on AIX servers](#) on page 113 for more information.
7. In the **UMASK** field, enter 007.
8. Select **Apply**.

Configuring resource settings

To configure WebSphere for the DB2 classpath, maximum heap size, and default encoding setting:

1. In the left frame of the Administrative Console, select **Servers > Application Servers**.
2. In the main frame, select **server1**.
3. Scroll down and select **Process Definition**.
4. Scroll down and select **Java Virtual Machine**.
5. In the **Classpath** field, enter the path to the DB2 JDBC 2.0 drivers. This will vary depending on how DB2 was installed. For the default **db2inst1** user, the path would be:

`/home/db2inst1/sqllib/java12/db2java.zip`
6. In the **Maximum Heap Size** field, enter 512.
7. Select **Apply**.
8. In the same frame, select **Custom Properties** at the bottom of the frame.
9. Select **New**.
10. In the **Name** field, enter:

`client.encoding.override`

Setting up Web servers

11. In the **Value** field, enter:

ISO-8859-1

12. Select **Apply**.

To configure WebSphere for the Thread Pool and the number of Keep Alive connections:

1. In the left frame of the Administrative Console, select **Servers > Application Servers**.
2. In the main frame, select **server1**.
3. Scroll down and select **Web Container**.
4. Select **Thread Pool**.
5. In the **Maximum** field, enter 100. This should be less than the value used for MaxClients when the HTTP Server software was installed. The default value for MaxClients is 150.
6. Select **Apply**.
7. In the same frame, select **Web Container** in the path at the top of the frame.
8. Scroll down and select **Custom Properties**.
9. Select **New**.
10. In the **Name** field, enter:
MaxKeepAliveConnections
11. In the **Value** field, enter 90.
12. Select **Apply**.

Removing the default application

The default application and the OA Reports application both use the default context root. To avoid collision, the default application must be removed.

To remove the default application:

1. In the left frame of the Administrative Console, select **Applications > Enterprise Applications**.
2. If the default application is present:
 - a. Select the default application name.
 - b. Select **Stop**.
 - c. Select the default application name again.
 - d. Select **Uninstall**.
3. Select **Save** on the main Administrative Console menu.
A verification dialog box is displayed.

4. Select **Save**.
5. Log out of the WebSphere Administrative Console.

Changing file permissions

To stop WebSphere and change the file permissions of WebSphere directories so that you can run as non-root user:

1. Log in as **root** at a terminal window.
2. Enter the following commands to stop WebSphere.

```
. ~INSTANCE_ID/.profile
cd $WEBSPPHERE_HOME/bin
./stopServer.sh server1
```

where *INSTANCE_ID* matches the ID used when the DB2 database instance was installed. The default instance ID is **db2inst1**.

3. Enter the following commands to change the file permissions, using the same user ID (*username*) and group ID (*groupname*) used earlier in this procedure (see [Prerequisites](#) on page 121):

```
chown -R username:groupname $WEBSPPHERE_HOME
chmod -R g+w $WEBSPPHERE_HOME/logs
chmod -R g+w $WEBSPPHERE_HOME/tranlog
chmod -R g+w $WEBSPPHERE_HOME/config
chmod -R g+w $WEBSPPHERE_HOME/temp
chmod -R g+w $WEBSPPHERE_HOME/wstemp
```

Starting WebSphere

To start WebSphere and verify it can be started as non-root user:

1. Enter the following commands:

```
. ~INSTANCE_ID/.profile
cd $WEBSPPHERE_HOME/bin
./startServer.sh server1
```

where *INSTANCE_ID* matches the ID used when the DB2 database instance was installed.

2. If this does not start, verify that the file permissions are correct as shown in Step [Changing file permissions](#) on page 127.

Setting up Web servers

3. For each failed restart, you must remove the WebSphere logs that are written as root.
Enter:

```
rm -fr $WEBSphere_HOME/logs/server1
```

4. If WebSphere or OA were previously started using the `root` user ID, enter the following commands:

```
chmod -R g+w /opt/BI/data/admin
```

```
chmod -R g+w /opt/BI/data/log
```

5. When WebSphere is running, enter the following command to see who owns the WebSphere process:

```
ps -ef | grep WebSphere
```

The process owner should be the user that started WebSphere. This must not be owned by `root`.

Changing the HTTP Server properties (optional)

If the IC Web Channel and the OA Report subsystem will be installed on the same server machine, there must be two instances of the IBM HTTP Server software installed on that machine (see [Prerequisites](#) on page 121 and [Installing WebSphere](#) on page 122). If a second instance of the HTTP Server software was installed, you must change the port number for the HTTP Server software and add the new port number to the virtual hosts using the WebSphere Administrative Console.



Important:

If you change the default HTTP Server port, users accessing the Report subsystem on this server must specify the new port number (for example, `http://machinename:portnumber/reports1` instead of using `http://machinename/reports1`).

If a second instance of the HTTP Server was not installed, you can skip this procedure.

Changing the HTTP Server port - To change the HTTP Server port number:

1. Enter:

```
cd /usr/INSTALL_PATH/conf
```

where `INSTALL_PATH` is the path where the HTTP Server software *was installed for* OA (for example, `/usr/OA_IBMHttpServer/bin`).

2. Enter:

```
vi httpd.conf
```

3. Search on the phrase "`Port 80`" and change it to an unused port number, for example, 81. The port selected cannot conflict with any ports used by Avaya IC or other OA applications.

4. Press **Esc**.

5. Enter:

:wq!

This writes and quits the file.

Adding the new HTTP Server port to the virtual hosts - To add the new HTTP Server port to the virtual hosts:

1. Using a browser window, enter:

`http://machinename:portnumber/admin`

where *machinename* is the server machine name where WebSphere is installed and *portnumber* is the new administration port number from [Changing the administration port](#) on page 122.

2. Log in with an administrator user ID.

3. In the left frame of the Administrative Console, select **Environment > Virtual Hosts**.

4. In the main frame, select **default host**.

5. Select **Host Aliases**.

6. Select **New**.

7. Enter * (an asterisk) in the **Host Name** field and 81 in the **Port** field.

8. Select **OK**.

9. Select **Save** twice.

10. In the left frame of the Administrative Console, select **Environment > Update Web Server Plugin**.

11. Select **OK**.

Creating a secure login by enabling Global Security (optional)

To apply password security to the Administrative Console:

1. Using a browser window, enter:

`http://machinename:portnumber/admin`

where *machinename* is the server machine name where WebSphere is installed and *portnumber* is the port number administered in [Changing the administration port](#) on page 122.

2. Log in with an administrator user ID.

3. In the left frame, select **Security > Global Security**.

4. In the main frame, select **Enabled**.

5. In the main frame, clear **Enforce Java 2 Security**.

Setting up Web servers

6. In the main frame, scroll down to **Active User Registry** and select **Local OS**.
7. In the main frame, select **Apply**.
8. In the left frame, select **System Administration > Console Users**.
9. Click on **Add**.
10. In the **User** field, enter the user ID you wish to use. This must match the user ID used during OA installation (for example, `biadmin`). See [Prerequisites](#) on page 121 for more information.
11. In the **Roles** field, select **Administrator**.
12. Select **Apply**.
13. Select **Save** on the main Administrative Console menu.
A verification dialog box is displayed.
14. Select **Save**.
15. If your configuration includes Avaya IC, install and configure Avaya IC as described in *Avaya Interaction Center Release 6.1 Installation and Configuration*.
16. Install OA by continuing with [Preparing for installation](#) on page 11 in *Avaya Operational Analyst Release 6.1 Installation and Configuration*.

■ ■ ■ ■ ■ ■

Appendix A: Time synchronization

Clocks on all server machines must be synchronized using a time synchronization package. The requirements for time synchronization is explained in [An explanation of time synchronization](#) on page 132.

For Windows 2000 systems, Tardis is one such package that has been tested successfully with OA. Tardis is shareware available at <http://www.kaska.demon.co.uk/>. See [Configuration tips for Tardis time synchronization on Windows](#) on page 136 for more information.



Important:

The customer is responsible for licensing this software.

For Sun Solaris systems, the NTPD process included with Solaris has been tested successfully with OA. See [Configuration tips for NTPD time synchronization on Solaris](#) on page 138 for more information.

For AIX, the NTPD process included with AIX has been tested successfully with OA. See [Configuration tips for NTPD time synchronization on AIX](#) on page 141 for more information.

An explanation of time synchronization

Time synchronization is the process of ensuring that the time-of-day clocks of all server machines within a defined network are set to the same time. This section discusses why time synchronization is important for Avaya IC and Avaya OA, the ramifications of not having time synchronization, and what is recommended to accomplish time synchronization.

Report data will be missing or inaccurate without time synchronization for Avaya IC and Avaya OA. Agent and queue/service class interval counts may not match, for example, if the related timestamps do not match. Data may not be available for reporting or negative durations may be computed if events are received out of order as a result of not having time synchronization.

Time synchronization is not a new requirement for Avaya Customer Relationship Management (CRM) products. Avaya CMS, for example, achieves time synchronization through the use of the Avaya Communication Manager software clock.

This section includes the following topics:

- [Need for time synchronization](#) on page 132
- [Customer prerequisites](#) on page 134
- [Service requirements](#) on page 134
- [Recommendations](#) on page 135
- [References](#) on page 135

Need for time synchronization

Avaya IC and Avaya OA can be deployed in multi-machine and multi-site environments. The multi-machine architecture allows a number of physical server machines to distribute the execution of the Avaya IC and Avaya OA processes. Given the distributed architecture of these products, time synchronization is critical for the generation of accurate timestamps so that events can be transformed properly into data items in the Avaya OA real-time database for storage and reporting.

Within Avaya IC, one server machine may handle agent records while another server machine may handle contact records. If the time-of-day clocks on these server machines are not synchronized then the timestamps associated with the contact will differ from the timestamps associated with the agent. This will result in either missing or inaccurate data being stored, summarized and reported by Avaya OA. Without time synchronization, for example, it is possible for Avaya OA to report an agent handling contacts while in auxiliary work mode (Aux Work).

In addition to inaccuracies between agent and contact data, there is also a risk of data being out of alignment when Avaya IC has queue/service class records on separate server machines from agent records. If the time-of-day clocks on these server machines do not match, then summarized data for queues/service classes may not match the summarized data for agents. For example, summarized data for an agent may indicate that the agent answered 37 contacts for a given queue/service class during a 30-minute interval while the queue/service class data may indicate slightly more or less. A time synchronization service can prevent errors such as this, but the granularity of the time synchronization service must be 0.5 seconds or less.

Other significant problems can occur when server machine clocks are not synchronized, such as negative durations on reports and missing data for some contacts. If the event indicating the end of a sequence has an earlier timestamp than the corresponding start event, Avaya OA will report a negative duration. Missing data can occur if events are processed out of sequence, which happens when Avaya OA reorders events based on timestamps. In this case, data for a particular contact may not be recorded because the events are processed before Avaya OA is aware that the contact has entered a certain state. These problems can be prevented if all server machines are running a time synchronization service, with a granularity of 0.5 seconds or less.

Outbound Contact is another component within the Avaya IC product. Outbound Contact writes data directly to the historical database. In this situation, the time associated with the Outbound Contact records must match the time associated with the separately recorded agent and contact records.

Troubleshooting can also be hindered when time is not synchronized across server machines. If the time-of-day clocks are not synchronized across server machines then the time recorded in error logs will not be synchronized. This complicates the debugging process and results in longer debugging times.

It is recommended that the Avaya IC and Avaya OA client desktops be synchronized to the same time as the Avaya IC and Avaya OA server machines. The Avaya IC client currently does record changes to agent states using the client time. Time synchronization on the Avaya IC client desktop, however, is not required since the Avaya IC client desktop is synchronized with an Avaya IC server machine at login. The Avaya IC and Avaya OA client desktops use the client time-of-day clock to timestamp error log entries when an error occurs on the client; therefore, having synchronized time on the client would aid the debugging process. An additional reason for synchronizing the client desktops, for example, is to ensure that the agent login/logout times match what is recorded for agent adherence applications and payroll applications.

As previously specified, Avaya IC and Avaya OA require a 0.5 second granularity of clock synchronization. This level of granularity will ensure that agent, outbound/inbound contact, queue/service class and error logging timestamps are synchronized. Without this level of granularity there is a risk that timestamps will not be aligned and customers will see erroneous data in their reports. For example, customers may see reports that show service levels that exceed 100%, negative durations, or numbers that don't add up properly. This will reduce the perceived reliability of the data and, therefore jeopardize the effectiveness of operating decisions.

Customer prerequisites

Avaya IC and Avaya OA customer prerequisites state that the customer must provide a time synchronization service on each server machine within the product configuration. The Avaya IC and Avaya OA products do not intrinsically provide time synchronization. It is the customer's responsibility to obtain the appropriate time synchronization packages and the associated licenses.

Many corporate firewalls do not permit the passage of NTP packets. If this is the case, there may be an existing time server behind the firewall that is configured with special permissions to synchronize with an external time server. In this scenario, the server that performs the external time synchronization would, in turn, be used as a host time server behind the firewall for other corporate servers. In a more sophisticated scenario, large companies may have an atomic clock time source, which is then used to drive a host time server. Two or more time servers would synchronize from the host server and each of these servers can feed subsequent time servers. This allows time synchronization clients on application servers to be configured for failover. In the case where a single time server becomes unavailable, the time synchronization client would immediately switch to another time server. Not all corporate environments, however, have the resources to provide this level of support. Therefore, it is necessary for each customer to determine a consistent time synchronization policy to ensure that time synchronization is always available for the Avaya IC and Avaya OA products.

Service requirements

The deployed time synchronization server machine must be accurate within 0.5 seconds.

The time synchronization service must be set up to initialize when the server machine is booted. If the time synchronization service is not started before the Avaya IC or Avaya OA processes that reside on the server machine, then there is the risk of timestamps being out of sync across servers.

The selected time synchronization service needs to ensure that all Avaya IC and Avaya OA deployed server machines within a configuration are synchronized based on Coordinated Universal Time (UTC), regardless of location, so that timestamps use UTC time. Additionally, time needs to be synchronized across Avaya OA and Avaya IC server machines regardless of operating systems. A Microsoft Windows 2000 server machine in Boston, for example, must be synchronized with Solaris server machines in Boston and London.

The time synchronization service must be reliable and must have high availability.

Recommendations

Network Time Protocol (NTP) is the time synchronization solution that is recommended for the server machines that support the Avaya IC and Avaya OA products. NTP claims to provide synchronization within several milliseconds on a LAN, allows for clock drift, avoids resetting the time in big “jumps,” and provides recovery capabilities when redundant clock sources are provided. NTP uses Coordinated Universal Time (UTC) and accounts for daylight savings time and time zones, assuming the time zone is set correctly on each machine. NTP has been in use for several decades, and many implementations of NTP are available, including versions for Windows NT, Windows 2000, Windows XP, Solaris, and AIX.

References

For more information on NTP:

- Introduction to NTP: <http://www.sun.com/blueprints/0701/NTP.pdf>
- NTP administration and architecture: <http://www.sun.com/blueprints/0801/NTPpt2.pdf>
- NTP monitoring and troubleshooting: <http://www.sun.com/blueprints/0901/NTPpt3.pdf>
- Latest information on NTP: <http://www.eecis.udel.edu/~ntp/>
- Search for NTP standards: <http://www.rfc-editor.org/overview.html>. For example, *Request for Comments (RFC) 1305: Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

Configuration tips for Tardis time synchronization on Windows

Tardis is an SNTP (Simple Network Time Protocol) time synchronization package available from <http://www.kaska.demon.co.uk/>. Avaya OA has been tested successfully using Tardis 2000 V1.4, which runs as a service on Windows 2000.



Important:

Even though Tardis is shareware, it is a commercial product and customers must be aware that there may be legal and trade agreement requirements. Customers may need to purchase an appropriate license for Tardis and are solely responsible for those licenses.

To ensure accurate time synchronization, install Tardis on every server machine and all data collection source servers. Configure it on each server machine as follows:

- **Main:** Do not use the default time servers that are preconfigured in Tardis. Instead, do one of the following:
 - If your company already has a reliable NTP time server, delete the pre-configured servers from the **Main** tab in Tardis and add your server.
 - If your company does not currently use NTP, you should designate one or more machines as time servers, and synchronize all other server machines to the time servers. The machines you designate as time servers should synchronize to a small number of reliable external time servers on the Internet, or to a hardware source, such as a global positioning system (GPS) receiver. You will need to experiment to determine which Internet time servers are reliable from your location, and delete all but those servers from Tardis. For the machines that you do not designate as time servers, delete all of the pre-configured servers from Tardis and add your local time servers.
- **General:** Select **Automatically change servers on failure**.
- **Setting the time:** Set Tardis to set the time with a minimum correction of 50 milliseconds, and a maximum correction of **Anything goes**. Set **How often the time is set** to 10 minutes, and select the **Adjust automatically** option.
- **Information:** Select **Log information messages**.
- **HTTP Proxy settings:** If you configure Tardis to connect to an Internet time server, you may need to set these.
- **Broadcast NTP/NTP:** Disable NTP broadcasts.
- **GPS:** If you are using a GPS receiver as a clock source, you will need to change these settings.



Important:

Other versions of Tardis have *not* been tested with OA. The K9 broadcast client that comes with Tardis has *not* been tested.

If you choose to use other time synchronization software, please ensure that it has the following qualifications:

- NTP (Network Time Protocol) or SNTP (Simple NTP) capability is strongly recommended. NTP and SNTP are standard protocols supported by a number of software packages on nearly every operating system.
- The software must be capable of keeping clocks in sync to better than 0.5 second accuracy.
- Computer clocks can drift several seconds over a short period of time. The time synchronization software should be capable of adjusting its synchronization interval dynamically. If not, you must set it to synchronize every one or two minutes to ensure sufficient synchronization.
- The software should be able to log each adjustment made to the clock to verify the installation. If you see adjustments larger than 0.5 second (500ms), the frequency of adjustment needs to be increased.
- NTP and SNTP are standard protocols so it is possible to mix and match different client and server software packages. However, if possible, you should use the same software package on all machines to simplify configuration.
- If the software has an option to automatically adjust the clock frequency, deselect or turn off that option.

Configuration tips for NTPD time synchronization on Solaris

All Solaris 8 and above operating systems have the NTPD software loaded, and are ready for being time synchronized within an NTPD infrastructure.

Solaris comes with the following sample NTP files (`/etc/inet/ntp.server` and `/etc/inet/ntp.client`), but without an actual `ntp.conf` file. Once the file `/etc/inet/ntp.conf` is in place, the script `/etc/init.d/xntpd` can be run to start the `xntpd` daemon. The `xntpd` daemon is run when the machine boots, then runs continuously keeping your server machine time synchronized with the other machines within your NTP infrastructure.

If you already have an NTP infrastructure, the `ntp.conf` file provided by your system administrator should be installed in `/etc/inet/`. If you do not already have an NTP infrastructure, you will need to create one so that your OA server machines can be kept synchronized. A good source of information that will help you understand NTP and how to implement the infrastructure you need on Solaris can be found in the documents *Using NTP to Control and Synchronize System Clocks*, a three part series by Deeths and Brunette. You can find these documents at:

- <http://www.sun.com/blueprints/0701/NTP.pdf>
- <http://www.sun.com/blueprints/0801/NTPpt2.pdf>
- <http://www.sun.com/blueprints/0901/NTPpt3.pdf>

This section includes the following topics:

- [Setting up an NTP infrastructure](#) on page 139
- [NTP Security](#) on page 140

Setting up an NTP infrastructure

Avaya recommends that you designate one or more machines on your network as local NTP servers and have the rest of the machines be NTP clients of these servers. The server `ntp.conf` file might look something like:

```
# Stratum 1 servers (at least 3 sources should be included)
server <global company server>
server <local gps server>
server <global gps server>
server <local company server>

# Stratum 2 peers (if any)
peer <local ntp server1>
peer <local ntp server2>
peer <remote ntp server>

# Drift file. Put this in a directory that the daemon can write to.
/etc/ntp.drift
```

The client `ntp.conf` file might look something like:

```
# Stratum 2 servers (from the server list above - again 3 sources
# should be included)
server <local ntp server1>
server <local ntp server2>
server <remote ntp server>

# Watch for multicast packets
multicastclient 224.0.1.1

# Drift file. Put this in a directory that the daemon can write to.
/etc/ntp.drift
```

The Stratum 1 servers listed in the server `ntp.conf` file connect directly to a reference clock that provides an accurate time source. These could include public NTP time servers on the internet or a GPS receiver. For a list of hardware vendors for reference clocks as well as a list of public NTP servers see <http://www.ntp.org>.

NTP Security

NTP does have the capability to have NTP clients and servers authenticate each other using **keys**. Keys enable the **xntpd** daemon to authenticate who is sending NTP requests and only accept request from an authenticated source. Access to NTP services can also be restricted using the **restrict** directive in the **ntp.conf** file. Details about how to use these facilities to setup a secure NTP infrastructure can be found in the document *Using NTP to Control and Synchronize System Clocks - Part II: Basic NTP Administration and Architecture*, by Deeths and Brunette at <http://www.sun.com/blueprints/0801/NTPpt2.pdf>.

The command **/usr/sbin/ntptrace** can be run to check the time source for your machine, as well as its stratum and time offset from the local host.

Configuration tips for NTPD time synchronization on AIX

All AIX 5.1L and above operating systems have the NTP software loaded and are ready for time synchronization within an NTP infrastructure. AIX provides a skeleton `/etc/ntp.conf` file. The skeleton `ntp.conf` file should be replaced with one configured for your environment.

If you already have an NTP infrastructure, the `ntp.conf` file provided by your system administrator should be installed in `/etc/ntp.conf`. If you do not already have an NTP infrastructure, you need to create one so that your OA servers can be kept in synchronization.

Once a newly-configured `ntp.conf` file is in place, the ntp daemon `/usr/sbin/xntpd` can be manually started using the following command:

```
startsrc -s xntpd
```

To set up the server to start `xntpd` automatically when the machine boots:

1. Enter:

```
vi /etc/rc.tcpip
```

2. Enter:

```
/xntpd
```

The portion of the file that has this line is displayed. It will look similar to the following:

```
# Start up Network Time Protocol (NTP) daemon
#start /usr/sbin/xntpd "$src_running"
```

3. Remove the `#` character at the beginning of the "start" line. The resulting change will look similar to the following:

```
# Start up Network Time Protocol (NTP) daemon
start /usr/sbin/xntpd "$src_running"
```

4. Write and quit the file.

Time synchronization

■ ■ ■ ■ ■ ■

Appendix B: Networking

To set up your network, do the procedures in the following sections:

- [Enabling TCP/IP networking](#) on page 144
- [Verifying DNS Resolution](#) on page 145

To ensure that changing IP addresses do not contribute to networking failures, be sure to assign dedicated IP addresses to your OA server machines. Using DHCP may result in a different IP address each time a server machine is rebooted. If this happens, the OA interface services and CORBA object interfaces may fail.

Enabling TCP/IP networking

All Avaya IC and OA server machines and client applications use TCP/IP to communicate. You need to enable TCP/IP networking on each machine in an Avaya IC and OA system.

By default, Windows and UNIX operating systems include TCP/IP networking on all machines with network cards. Typically, Avaya IC and OA uses the default TCP/IP settings applied during installation.

However, if you deploy Avaya IC and OA on an existing Novell NetWare network, you may need to take additional steps to configure the TCP/IP networking protocol. You can obtain information on how to install and configure TCP/IP networking on a NetWare network from your IT professionals.

Verifying DNS Resolution

Before you install the historical database on the server machine, you must verify the Domain Name System (DNS) resolution on each machine.

Each server machine must have a fully-qualified domain name that:

- Has a minimum of three parts, separated with periods. For example, `bsmith.com` only has two parts and does not qualify as a fully-qualified domain name. The name `bsmith.domain.com` has three parts and does qualify as a fully-qualified domain name.
- Does not contain special characters, except the dash (-).
- Has forward and reverse DNS mapping in public DNS records.

Record the information after you verify each machine's DNS resolution. You can use the `ping` command to test connectivity between machines.

This section includes the following topics:

- [Verifying DNS Resolution in Windows](#) on page 146
- [Verifying DNS Resolution on Solaris](#) on page 147
- [Verifying DNS resolution on AIX](#) on page 148
- [Troubleshooting an Unresolved DNS Entry](#) on page 149

Verifying DNS Resolution in Windows

The following procedure verifies that the fully-qualified domain name is configured properly for Windows. Perform this procedure on every server machine that has a Windows operating system.

To verify DNS resolution in Windows:

1. Open a command window.
2. Find the IP address of the machine. Enter the following command at the prompt:

```
ipconfig
```

The system returns information about the machine's IP configuration, including the IP address, as shown in the following example:

```
Windows IP Configuration
Ethernet adapter El70x1:
IP Address. . . . . : 254.24.167.211
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 254.24.167.1
```

3. Verify the *reverse* DNS mapping. Enter the following command with the machine's IP address at the prompt:

```
nslookup <IP_address>
```

The system returns information about the machine's reverse DNS mapping, as shown in the following example:

```
Server: ns3.domain.com
Address: 254.24.167.23
Name: bsmith.domain.com
Address: 254.24.167.211
```

4. Verify the *forward* DNS mapping. Enter the following command with the machine's fully-qualified domain name at the prompt:

```
nslookup <machine_name>.<domain_name>
```

The system returns information about the machine's forward DNS mapping, including the machine's IP address and fully-qualified domain name. The following example of forward DNS mapping indicates that the fully-qualified domain name `bsmith.domain.com` is assigned to the IP address `254.24.167.211` in public DNS records.

```
Server: ns3.domain.com
Address: 254.24.167.23
Name: bsmith.domain.com
Address: 254.24.167.211
```

Verifying DNS Resolution on Solaris

The following procedure verifies that the fully-qualified domain name is configured properly for Solaris. Perform this procedure on every server machine with a Solaris operating system.

To verify DNS resolution on Solaris:

1. Enter:

```
cd /etc
```

2. Open the `hosts` file and locate the information about the machine's IP configuration, including the IP address.
3. Verify the *reverse* DNS mapping. Enter the following command with the machine's IP address at the prompt:

```
nslookup <IP_address>
```

The system returns information about the machine's reverse DNS mapping, as shown in the following example:

```
Server: ns3.domain.com
Address: 254.24.167.23
Name: bsmith.domain.com
Address: 254.24.167.211
```

4. Verify the *forward* DNS mapping. Enter the following command with the machine's fully-qualified domain name at the prompt:

```
nslookup <machine_name>.<domain_name>
```

The system returns information about the machine's forward DNS mapping, including the machine's IP address and fully-qualified domain name. The following example of forward DNS mapping indicates that the fully-qualified domain name `bsmith.domain.com` is assigned to the IP address `254.24.167.211` in public DNS records.

```
Server: ns3.domain.com
Address: 254.24.167.23
Name: bsmith.domain.com
Address: 254.24.167.211
```

Verifying DNS resolution on AIX

The following procedure verifies that the fully-qualified domain name is configured properly for AIX. Perform this procedure on every server machine with an AIX operating system.

To verify DNS resolution on AIX:

1. Enter:

```
cd /etc
```

2. Open the `hosts` file and locate the information about the machine's IP configuration, including the IP address.
3. Verify the *reverse* DNS mapping. Enter the following command with the machine's IP address at the prompt:

```
nslookup <IP_address>
```

The system returns information about the machine's reverse DNS mapping, as shown in the following example:

```
Server:  ns3.domain.com
Address:  254.24.167.23
Name:     bsmith.domain.com
Address:  254.24.167.211
```

4. Verify the *forward* DNS mapping. Enter the following command with the machine's fully-qualified domain name at the prompt:

```
nslookup <machine_name>.<domain_name>
```

The system returns information about the machine's forward DNS mapping, including the machine's IP address and fully-qualified domain name. The following example of forward DNS mapping indicates that the fully-qualified domain name `bsmith.domain.com` is assigned to the IP address `254.24.167.211` in public DNS records.

```
Server:  ns3.domain.com
Address:  254.24.167.23
Name:     bsmith.domain.com
Address:  254.24.167.211
```

Troubleshooting an Unresolved DNS Entry

If a DNS entry is not set up for an OA server machine, you can temporarily use local host entries.

Note:

This workaround is only temporary. You must establish true DNS resolution as quickly as possible for an easier implementation.

To add local host entries for the servers:

1. Open the `hosts` file in a text editor.
 - Windows default location: `\WinNT\System32\Drivers\etc`
 - Solaris and AIX default location: `/etc`
2. In the `hosts` file, locate the IP entry and name for `localhost`.

For example, the `localhost` line in the file might read:

```
127.0.0.1      localhost
```

3. Add an entry for each machine:
 - a. Look for the line that has `localhost`. At the end of the `localhost` line, press **Enter** to get a new line.
 - b. Enter the machine's IP address.
 - c. Press **Tab** or enter a few spaces, and enter the machine's fully-qualified domain name.
 - d. Press **Tab** or enter a few more spaces, and enter the machine name.

The machine name and the fully-qualified domain name resolve to the specified address, as shown in the following example:

```
192.168.0.1      <machine_name>.<domain_name>      comhub
192.168.0.2      <machine_name>.<domain_name>      sql
```

4. Save the file under its original name (`hosts`).

Note:

If the IP address changes, you must update the `Hosts` file to reflect this change.

Glossary

ADU	Agent data unit
back-end database	A historical database that is located on a different machine than where the Historical subsystem software is installed.
base interval	OA lumps IC real-time data into 30-minute intervals in the Historical subsystem. Also called intervals. See also base interval data.
base interval data	Real-time data that OA has lumped into 30-minute intervals. The Real-time subsystem summarizes IC data into 30-minute intervals and transfers it to the Historical subsystem, which proceeds to aggregate the base interval data into containers.
communication server	The equipment that provides telecommunications service to agents and supervisors in a contact center.
container	Metadata that defines how data should be sifted and stored in the historical database. The term "container" encompasses both the table definition as well as the data contained in the table.
Customer Information Repository	The IC and OA databases in an Avaya IC and Avaya OA system.
EDU	Electronic Data Unit
FQDN	Fully-qualified domain name
historical database	The main database used by Avaya OA, Avaya IC, and CMS. There can be only one historical database.
historical server	The server where the Historical subsystem is installed.
RAID	Redundant Array of Inexpensive Disks

real-time database

real-time database The database that collects data from Avaya IC subsystems. This database is used for real-time reports and sends summary data to the historical database.

server machine The physical computer where software is installed.

Sun ONE Web Server The new product name for the Solaris Web server, formerly iPlanet.

TNS Transparent Network Substrate

Web container The web servlet engine that is used by the Web server software.

Index

A

- administering
 - WebSphere to run as a non-root user 125
- Advanced Report server 39
- Avaya Business Advocate considerations 26
- Avaya IC
 - considerations 26
 - server configuration 26
- Avaya IC filegroups or tablespaces (required with Avaya IC tables). 56
- Avaya OA components. 12

B

- basic report server. 38

C

- changing
 - file permissions 127
 - HTTP Server properties (optional). 128
 - WebSphere administration port 122
- client applications
 - hardware requirements 29
 - software requirements 32
- client PC minimum hardware requirements 29
- client software requirements 32
- CMS
 - considerations 27
 - server configuration 27
- CMS filegroups or tablespaces (required with CMS tables) 55
- Cognos
 - utilities. 49
- common filegroups or tablespaces (required for OA). 55
- configuration 21
 - Avaya IC server considerations 26
 - CMS server considerations 27
 - database server considerations 24
 - Real-time database server considerations 25
 - report server considerations. 25
 - SQL server 2000 64
- tips
 - NTPD time synchronization (Solaris). 138
 - Tardis time synchronization (Windows). 136
- configuration tips
 - NTPD time synchronization (AIX) 141
- configuring

- DB2 database tunables 97
- locale settings in Solaris 110
- message logging 112, 114
- Oracle database instance on Solaris 84, 89
- Oracle database instance on Windows 78
- Real-time subsystem locale settings on Windows 107
- Real-time subsystem parameters 111, 114
- semaphores 111
- SQL server 2000 64
- tablespaces on DB2. 99
- considerations 22
 - database 22
 - general. 22
 - historical database 23
 - server 22
- creating
 - database instance on AIX 94
 - group IDs. 106, 108, 113
 - Oracle database instance on Solaris 84, 89
 - Oracle database instance on Windows 71, 78
 - secure login by enabling Global Security (optional) 129
 - SQL server 2000 back-end database. 65
 - tablespaces on Solaris 85, 90
 - tablespaces on Windows 72, 78
 - user IDs 106, 108, 113
- Creating an SQL Server 2000 back-end database . . 65

D

- database 22
 - configurations 57
 - considerations 23
 - install 53
- Oracle
 - create on Solaris 84, 89
 - create on Windows 71, 78
 - planning 15
 - server configuration 24
 - SQL server 2000
 - create. 65
- DB2 limit on SQL statement length 46
- default gateway 146
- determining
 - system size and configuration 21
- DNS
 - unresolved 149
 - verifying on Solaris 147, 148
 - verifying on Windows 146
 - verifying resolution 145

domain name system 145

E

enabling
 TCP/IP networking 144

F

features 12
filegroup and tablespace sizing 55
finding IP addresses 146
fully-qualified domain name 145

G

glossary 151

H

hardware requirements 29
 client 29
 server 30
historical database software 45
historical server
 considerations 24
 coresident database 35
 without coresident database 36
Historical subsystem
 coresident with the historical database 35
 not coresident with the historical database 36
hosts file 149

I

installing
 database 53
 DB2 administration client software 101
 DB2 administration client software on AIX 100
 DB2 database server software 95
 DB2 on AIX. 91
 DB2 software 94
 historical database 53
 IIS Web server on Windows 118
 Microsoft SQL Server 2000 on Windows 60
Oracle
 Solaris 84, 89
 Solaris client 85, 90
 Windows client 73, 79
Oracle 8.1.7 database client on Solaris 85, 90
Oracle 8.1.7 database client on Windows 73, 79
Oracle 8.1.7 database server on Solaris 84, 89

Oracle 8.1.7 database server on Windows 71, 77
Oracle 8i on Solaris 81
Oracle 8i on Windows 68
Oracle 9i database client on Solaris. 90
Oracle 9i database client software on Windows 79
Oracle 9i database server software on Solaris 89
Oracle 9i database server software on Windows. 77
Oracle 9i on Solaris 86
Oracle 9i on Windows 74
Solaris patches 43
SQL server 2000 60
SQL server 2000 server and client tools. 63
Sun ONE Web server (formerly iPlanet). 119, 121
Sun ONE Web server on a Solaris server 119, 121
WebSphere 122
Installing and configuring WebSphere on an AIX machine
 121
Installing the historical database software 53
introduction 11
IP address 146

J

Java Run-time Environment 50
Java utilities 49, 50

L

localhost 149

M

Microsoft SQL server 2000 45

N

networking 51, 143
 Novell network 144
 TCP/IP 144
Novell network 144
nslookup 146, 147, 148
NTP security 140

O

OA filegroups or tablespaces 55
operating system 42
Oracle 45
 create database on Solaris 84, 89
 create database on Windows. 71, 78
 install client on Solaris 85, 90
 install on Solaris 84, 89

installation	
Windows client	73, 79
Solaris	81
Windows	68
organization	8

P

partitioning	43
path definitions	122
planning checklist	14
platform requirements	15, 29, 31
preface	7
product description	7

R

RAID configurations	30
Real-time	
database server configuration	25
server considerations	25
reasons for reissue	8
related information	9
report server	
configuration	25
considerations	25
requirements	
platform	15, 29, 31
software	33

S

s	57
sample historical database layout	58
security	51
server	
configuration	
Avaya IC considerations	26
CMS considerations	27
database considerations	24
Real-time database considerations	25
report server considerations	25
configurations	16
considerations	22
hardware requirements	30
planning	15
software requirements	33
server machine hardware sizing	30
setting	
database alias	101
DB2 registry values and environment	96
NTP infrastructure	139

software	
considerations	42
required for historical servers	34
required for Real-time servers	37
required for report servers	38
required for source-CMS collection subsystem	40
required for source-EC (Event Collector) collection subsystem	40, 41
required for Source-EC Bridge (Event Collector Bridge) collection subsystem	41
requirements	33
client	32
system-level	42
Web server	44
software considerations	50
software requirements	31
Solaris	
patches	43
requirements	42
verifying DNS resolution	147, 148
SQL server 2000	45
configure	64
create database	65
install	60
starting	
Administrative Console	124
WebSphere	124, 127
subnet mask	146
Sun ONE Web server (formerly iPlanet)	119, 121
swap space	44
system size	21

T

TCP/IP networking	144
time synchronization	51, 131
Solaris	138
Windows	136
TimesTen software	49
troubleshooting	
DB2 installation	103
unresolved DNS	149
unresolved DNS entry	149

U

user ID creation	106, 108, 113
----------------------------	---------------

V

verifying	
DNS resolution	145

AIX	148
Solaris	147, 148
Windows	146
virus scan software.	50

W

Web server software	44
Windows	
verifying DNS resolution.	146