

# Best Practices for Cisco Secure ACS for UNIX Administration

Document ID: 63755

---

**Introduction**

**Prerequisites**

Requirements

Components Used

Conventions

**Listing of Best Practices**

Steps

**NetPro Discussion Forums – Featured Conversations**

**Related Information**

---

## Introduction

This document provides the best practices for administrating the Cisco Secure (CS) ACS for UNIX application. The recommendations presented in this document are based on design and deployment experiences by Cisco Development Engineers (DE).

## Prerequisites

### Requirements

Readers of this document should have knowledge of these topics:

- configuring and administering CS ACS for UNIX

### Components Used

The information in this document is based on these software and hardware versions:

- CS ACS UNIX version 2.3(5)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

## Listing of Best Practices

Below is a listing of the recommended best practices.

## Steps

Complete these steps:

1. Make sure that the SqlAnywhere database does not exceed 5000 user profiles.
2. Accounting records should not exceed 50,000 records in the accounting tables.
3. Run the AcctExport utility daily.
4. If the transaction rate is very high, and there is huge accounting traffic such that there are more than 50,000 accounting records, then run AcctExport twice or thrice based on the load.
5. Make sure that there is adequate disk and Swap space available on the Solaris box.
6. Run the dbunload utility monthly. This will help to reduce the size of CSUnix Database.
7. The csecure.db should never exceed 1 GB of disk space.
8. If the csecure.db exceeds in size very quickly, then make sure that dbunload is run more frequently.
9. If Radius AAA is not used in CS, then this can be disabled with the help of R flag in /etc/rc2.d/S80Ciscosecure.
10. At runtime, DBServer errors, including the errors encountered in the interface to database, are reported in the logfiles/csdb\_ <date> file. Any unexpected errors or crash information by JAVA Virtual Machine are logged in log/dbserver.log file. Check these files for any errors.
11. If the AAAServer crashes, the core files will be located in the \$BASEDIR/corefiles. Check for the existence of core files, if any.
12. Backup the database regularly (daily or weekly), based on the customers' needs.
13. For better performance, disable the csuslog logging feature. This will drastically increase the performance.
14. The ulimit value should be 4096 in /etc/system, /etc/rc2.d/S80Ciscosecure \$BASEDIR/bin/DBServer.sh
15. Remove the csecure.log regularly. Before removing the csecure.log, CS should be stopped.
16. Do not manually add/modify/delete the database/ tables directly – use only the supported methods.
17. Archive the \$BASEDIR/logfiles directory once a month.
18. Archive /var/log/csuslog files regularly, and trim the size by issuing the command **cat /dev/null > csuslog**. If the file is deleted, syslog will not work, and hence the log will not be redirected to the csuslog file.
19. DNS Server Issues: If the target system has a DNS configured, or if the Solaris operating system has been configured as a DNS server, special care must be taken to insure that DNS performance and operations are fully operational.

If the CS ACS server target Solaris system has DNS enabled, there might be performance or authentication issues for CS ACS. CS ACS does not directly call a DNS server; however, the Solaris operating system calls gethostbyadd\_r and might indirectly call the DNS server, if configured to do so. Check the /etc/nsswitch.conf file for such a configuration. If the DNS domain name resolution operation does not work or is slow, this directly affects CS ACS.

20. While running tools such as dbbackup and dbunload, the PATH should be correctly set. Otherwise, the tools may not work properly. \$BASEDIR/utills/bin/env\_setup can be used for setting the path. This file contains all of the required environmental variables and other path details.
21. The MaxConnection and ConnectionLicense parameters should be set so as to meet the needs based on the number of authentications and the number of Transactions that the CSU can handle. MaxConnection can be set to a max value of 50, if the db used is SqlAnywhere. Increase the ConnectionLicense in \$BASEDIR/config/CSConfig.ini, and correspondingly increase the value of MaxConnection in \$BASEDIR/CSU/libdb.conf to a value two less than the ConnectionLicense based on the load.
22. When using automated scripts to log in to routers and switches, and execute commands, it is a good practice to place **sleep** commands in between regular router/switch commands. This helps spread the load and avoid resource contentions in the CS server.
23. Further, these automated scripts should properly close Telnet sessions (even in the case of any command failures) to ensure resources are not locked at the CS server.

# NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

## Related Information

- [CiscoSecure ACS for UNIX, 2.3\(5\) Technical Documentation](#)
- [Cisco Secure Access Control Server for Unix Product Support](#)
- [Technical Support – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 19, 2006

Document ID: 63755

---