Software Product Description

Product Name: **POLYCENTER Security Compliance Manager for SunOS, Version 2.4** **SPD 41.25.02**

DESCRIPTION

In previous versions of POLYCENTER™ Security products, the name DECinspect™ was used instead of POLYCENTER Security.

POLYCENTER Security Compliance Manager (POLYCENTER Security CM) for SunOS® is a software tool that a security or system manager uses to establish a custom security analysis and reporting system to manage the security of a network of distributed systems. With this tool, the security manager can implement and maintain a security standard for the SunOS nodes in a distributed computing environment that is consistent with corporate security policy.

Customers can purchase security consulting services that help them to design and implement a security analysis and reporting system, which balances business needs with security requirements. Local Digital™ offices can help customers to determine the appropriate services for their requirements.

Security managers define tests to examine the settings of operating system parameters that are relevant to the security of the system. These tests ensure that the operating system parameters comply with the organization's security policy. Using POLYCENTER Security CM's menu interface, these tests are grouped into inspectors, which are run regularly to test for compliance with the security policy.

POLYCENTER Security CM provides tests to examine the following categories of system settings:

- File and directory protections
- Accounts
- Passwords
- Network access
  - TCP/IP
  - UUCP
  - Remote login
  - NFS®
- Auditing

Inspectors arrange tests hierarchically into subsystems, test collections, and tests. The system settings that POLYCENTER Security CM tests are defined as parameters for the tests within the inspector. When POLYCENTER Security CM executes inspectors, it generates the following:

- Reports — POLYCENTER Security CM mails reports, summarizing the results of the inspection, to a distribution list specified for each inspector.
- Lockdown scripts — POLYCENTER Security CM generates lockdown scripts that can be used to automatically reset parameters that do not comply with the requirements of the inspector.
- Unlockdown scripts — POLYCENTER Security CM generates unlockdown scripts that can be used to reverse the operation of the corresponding lockdown file. POLYCENTER Security CM generates a corresponding unlockdown script every time it generates a lockdown script. POLYCENTER Security CM also creates a corresponding unlockdown log file.
- Tokens — POLYCENTER Security CM generates tokens after executing a special type of inspector. This inspector is called the Required Inspector and is described in the following paragraph. Tokens contain summaries of the results of the Required Inspector. POLYCENTER Security CM transmits these tokens to a POLYCENTER Security Reporting Facility (POLYCENTER SRF) node. POLYCENTER SRF extracts the data from the tokens and stores it in a relational database. Designated users can access this information to monitor the security compliance of all the nodes in a network.

There are two types of inspectors: the Required Inspector and customized inspectors.

The Required Inspector is the inspector that POLYCENTER Security CM uses to test the compliance of the system with the security baseline in force. It defines the basic security settings that are required for compliance with an organization's baseline security standard. The POLYCENTER Security CM database contains at most one Required Inspector on each system. The database also contains several sample inspectors.

Customized inspectors do not generate tokens, but the local system manager uses them for specialized testing.

The following list describes some situations in which customized inspectors may be useful:

- Before executing the Required Inspector — If the Required Inspector is copied to a customized inspector, the system's security compliance can be tested without sending tokens to the POLYCENTER SRF node. Users can correct security weaknesses before POLYCENTER Security CM performs an inspection using the Required Inspector.
- After installing or upgrading the operating system.
- To inspect the system after changes in system software, resources, or utilities.
- When it is discovered that a user is accessing the system during unusual hours.
- When inexplicable modifications to file protections are discovered.
- When security compromises are suspected — Inspect the system using a customized inspector if daily audit reports reveal suspicious security events.
- To check project file and directory permissions — Project managers who are responsible for security in their particular area can use a customized inspector to check file and directory permissions for their area.

While POLYCENTER Security CM is effective when used alone in small distributed systems, managing the security of a large number of nodes is difficult. POLYCENTER Security CM software, used with POLYCENTER SRF software, can solve this problem. POLYCENTER SRF software is designed to run on one or more nodes to support the centralized collection and management of compliance information from POLYCENTER Security CM installations, which can include AIX®, HP®-UX, SunOS, ULTRIX™, Solaris® 2, DEC OSF/1® AXP™ and OpenVMS™ systems. It provides centralized management for distributed POLYCENTER Security CM client nodes. POLYCENTER SRF extracts data from tokens sent by nodes running POLYCENTER Security CM and maintains this data in a relational database for management reporting. POLYCENTER SRF can provide management reports for networks of AIX, HP-UX, SunOS, ULTRIX, Solaris 2, DEC OSF/1 AXP and OpenVMS nodes. For more information about managing network security, see the POLYCENTER SRF Software Product Description (SPD 26.N2.xx).

Additional Security Products

The following is a list of related security products:

- POLYCENTER Security Compliance Manager for OpenVMS (SPD 26.N1.xx)
- POLYCENTER Security Compliance Manager for ULTRIX (SPD 41.26.xx)
- POLYCENTER Security Compliance Manager for AIX (SPD 46.11.xx)
- POLYCENTER Security Compliance Manager for HP-UX (SPD 46.12.xx)
- POLYCENTER Security Compliance Manager for Solaris 2 (SPD 55.87.00)
- POLYCENTER Security Compliance Manager for DEC OSF/1 AXP (SPD 55.86.00)
- POLYCENTER Security Reporting Facility for OpenVMS (SPD 26.N2.xx)
- POLYCENTER Security Intrusion Detector for OpenVMS (SPD 41.27.xx)
- POLYCENTER Security Intrusion Detector for SunOS (SPD 43.09.xx)
- POLYCENTER Security Intrusion Detector for ULTRIX (SPD 43.07.xx)

HARDWARE REQUIREMENTS

The processor and hardware configurations that you need to run POLYCENTER Security CM are specified in the *System Support Addendum* (SSA 41.25.01-x).

SOFTWARE REQUIREMENTS

To run POLYCENTER Security Compliance Manager for SunOS, you must be running SunOS Operating System Version 4.1.1 or higher.

See the System Support Addendum (SSA 41.25.01-x) for information on the availability and required versions of the prerequisite and optional software.

ORDERING INFORMATION

Software Licenses QL-MLCA*-**
Software Media: QA-MLCA*-**
Software Documentation: QA-MLCAA-GZ
Software Product Services: QT-MLCA*-**

* Denotes variant fields. For additional information on available licenses, services, and media, see the appropriate price book.

SOFTWARE LICENSING

This software is furnished under the licensing provisions of Digital Equipment Corporation's Standard Terms and Conditions. For more information about Digital's licensing terms and policies, contact your local Digital office.

Possession, use, or copying of the software described in this publication is authorised only pursuant to a valid written licence from Digital or an authorised sublicensor.

SOFTWARE PRODUCT SERVICES

A variety of service options are available from Digital. In addition to standard SPS remedial services, consulting services to help plan, design, and implement a custom security analysis and reporting system with the POLYCENTER Security CM and POLYCENTER SRF tools are also available. For more information, contact your local Digital office.

SOFTWARE WARRANTY

Warranty for this software product is provided by Digital with the purchase of a license for the product as defined in the Software Warranty Addendum of this SPD.

® AIX is a registered trademark of International Business Machines Corporation.

® HP is a registered trademark of Hewlett-Packard Company.

® NFS, Solaris and SunOS are registered trademarks of Sun Microsystems, Inc.

® OSF and OSF/1 are registered trademarks of the Open Software Foundation Inc.

™ SPARCstation is a registered trademark of Sun Microsystems, Inc.

™ The DIGITAL logo, AXP, DEC, Digital, OpenVMS, POLYCENTER, ULTRIX, and VMS are trademarks of Digital Equipment Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

System Support Addendum

Product Name: POLYCENTER Security Compliance Manager for SunOS, Version 2.4 **SSA 41.25.02-A**

In previous versions of POLYCENTER™ Security products, the name DECinspect™ was used instead of POLYCENTER Security.

HARDWARE REQUIREMENTS

Processors Supported

POLYCENTER™ Security Compliance Manager (POLYCENTER Security CM) for SunOS® supports all SPARCstations™ and SPARCservers.

Other Hardware Required

To install POLYCENTER Security Compliance Manager for SunOS software, the system must support a tape drive suitable for QIC-150 tapes.

Disk Space Requirements

Disk Space Required for Installation

/usr/kits/SSS240:	2,500K bytes
/usr/var/kits/SSS240:	1,000K bytes
/usr/kits/SSS240/man:	10K bytes
Any directory:	2,500K bytes

Disk Space Required for Use (Permanent)

/usr/kits/SSS240:	2,500K bytes
/usr/var/kits/SSS240:	1,000K bytes
/usr/kits/SSS240/man:	10K bytes

All of these directories can be links to other local or NFS®-mounted file systems.

The sizes are approximate; actual sizes may vary depending on the user's system environment, configuration, and software options.

SOFTWARE REQUIREMENTS

SunOS Operating System Version 4.1.1 or higher

GROWTH CONSIDERATIONS

The minimum hardware/software requirements for any future version of this product may be different from the requirements for the current version.

DISTRIBUTION MEDIA

18-track QIC-150 streaming tape

ORDERING INFORMATION

Software Licenses: QL-MLCA*-**
Software Media: QA-MLCA*-**
Software Documentation: QA-MLCAA-GZ
Software Product Services: QT-MLCA*-**

* Denotes variant fields. For additional information on available licenses, services, and media, see the appropriate price book.

The above information is valid at time of release. Please contact your local Digital office for the most up-to-date information.

® AIX is a registered trademark of International Business Machines Corporation.

® HP is a registered trademark of Hewlett-Packard Company.

® NFS, Solaris and SunOS are registered trademarks of Sun Microsystems, Inc.

® OSF and OSF/1 are registered trademarks of the Open Software Foundation Inc.

™ SPARCstation is a registered trademark of Sun Microsystems, Inc.

™ The DIGITAL logo, AXP, DEC, Digital, OpenVMS, POLYCENTER, ULTRIX, and VMS are trademarks of Digital Equipment Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

March 1994
AE-PQ1WC-TE