Cyclades™ ACS 5000 Advanced Console Server Appliances
Release Notes
Version 3.3.0-6
February 17th 2011

This document outlines:

1. Update Instructions
2. Appliance Firmware Version and Language Support Information
3. Enhancements
4. Fixes
5. Known Issues / Restrictions
6. Configuration Details

==========

Update Instructions

==========

Please refer to your installation, administrator and user manual for detailed instructions to update the Cyclades ACS 5000 console server to version 3.3.0-6.

In order to have all features listed in this release available through DSView™ 3 management software, DSView 3 software version 3.7.1 and the Cyclades ACS 5000 console server plug-in version 3.3.3 are required. An appliance firmware package to upgrade from DSView 3 software is also available.

After Cyclades ACS 5000 console server firmware has been upgraded to version 3.3.0-6, it is mandatory that the Web browser cache of any system which intends to be connected to the Cyclades ACS 5000 console server Web interface is cleaned up.

Cyclades ACS 5000 console server firmware version 3.3.0-6 provides an internal mechanism which preserves existing configuration when upgrading from firmware versions 1.0.2 and later. However, it is strongly recommended that you back-up system configuration before the firmware version is upgraded.

==========

Appliance Firmware Version and Language Support Information

==========

Appliance/Product	**Firmware Type**	**Version**	**Filename**	**Part Number**
Cyclades ACS 5000 console server (all models)	Opcode	V_3.3.0-6	FL0588-005.bin FL0588-005.bin.md5 FL0588-005.pkg	FL0588-005

English language supported.

==========

Enhancements

==========

Please refer to your installation, administrator and user manual for a detailed list of features supported by the Cyclades ACS 5000 console server version 3.3.0-6.

Major features of the Cyclades ACS 5000 console server 3.3.0-6 include:

I. **Security Profile –** Provide preset security profiles (secure, moderate and open) and the flexibility for IT managers to customize security profiles in order to comply with existing network security policies, as supported by the Cyclades™ ACS Advanced Console Server

II. **New Authentication Services** – The following authentication services are supported by the Cyclades ACS 5000, as supported by the Cyclades ACS Advanced Console Server:

    1. Kerberos™ Authentication
    2. Two-factor authentication (RSA SecurID® authentication)
    3. OTP (One Time Password)
    4. NIS Authentication

III. **Group Authorization** – Support authorization based in group access right, as supported by the Cyclades ACS Advanced Console Server. The group that the user belongs to can be specified by remote authentication servers: RADIUS, TACACS+ and LDAP.

IV. **Dual Stack support with IPv4 & IPv6** - Both IPv4 and IPv6 protocols are concurrently supported, as supported by the Cyclades ACS Advanced Console Server. As a result of this addition, a few other enhancements were added which are listed below:

1. ICMPv6 support.
2. DHCPv6 support: Ethernet IPv6 addresses can be dynamically assigned by a DHCPv6 server.
3. Stateless auto-configuration support.
4. The following remote authentication services support IPv6:
    - DSView
    - RADIUS
    - TACACS+
    - LDAP
    - Kerberos™
5. Serial interfaces can be configured with IPV6 addresses (port IP alias).
6. PPP interfaces can be configured or dynamically assigned with IPv6 addresses. This refers to serial ports with external modems and PCMCIA analog modem cards using the PPP protocol. PCMCIA ISDN cards do not support IPv6.

7. The following networking services can be configured to support IPV6 protocol:
    a. Access to DNS Servers
    b. Sending messages to Syslog Servers
    c. SNMP
    d. Sending SNMP Trap
    e. Remote Authentication (see item 4 for further details)
    f. Access to Hosts
    g. Stateful and stateless packet filtering (firewall)
    h. Static Routes
    i. Sending messages/events to SMTP Servers
    j. Sending data to Data Buffering Servers
    k. Access to NTP Server
    l. FTP (file transfer) for Configuration Backup
    m. FTP (file transfer) for Firmware upgrade

V. **Linux® kernel upgrade:** upgraded the Linux kernel from version 2.6.11.12 to version 2.6.22.1 and enabled IPv6 support.

VI. **IPSec support:** IPSec with NAT transversal supported as in the Cyclades ACS Advanced Console Server.

VII. **IPMI:** IPMI Power Management support as supported by the Cyclades ACS Advanced Console Server.

VIII. **Mindterm support:** Mindterm terminal emulator version 3.1.2 is now used to launch serial port sessions using SSH or telnet protocols.

IX. **Radius Service Type support:** Implemented support to this Radius attribute. When the feature is enabled and "service_type" attribute value is 6 (six), the Cyclades ACS 5000 console server shall recognize the user as an "administrator" (a member of the internal Cyclades ACS 5000 console server "admin" group).

X. **Power Management Enhancements:**

1. Support new Avocent Power Management Distribution Unit: PM 1000, PM 2000 and PM 3000 families, and ServerTech Smart CDU™ with version 6.0g or later.

2. pmCommand has new commands to support the measured information of the new IPDU.

XI. **Web User Interface (OBWI) Enhancements** – new pages to add the configuration of the new features as the Cyclades ACS Advanced Console Server OBWI.

1. PDU Power Mgmt menu: new pages to support the measured information of the PDUs.
2. IPMI Power Mgmt menu: IPMI servers configuration
3. Host Settings: IPv6 configuration
4. VPN Connections: IPSec configuration
5. Authentication: Kerberos™ and NIS server's configuration
6. Security Profile page instead of Services page.
7. System Information shows the unit Serial Number.

XII. Enterprise MIB: Enterprise MIB were extended to add PDU information and IPv6 information. Some OIDs are obsolete in this release.

XIII. OpenSSL Upgrade: Upgrade to 0.9.8l because of security vulnerability CVE-2009-3555.

XIV. OpenSSH Upgrade: Upgrade from 4.4.p1 to 5.6p1. Support for Kerberos™TGT as supported by Cyclades ACS Advanced Console Server.

XV. Update on the Avocent Certificate used by java applet on 'Connect'.

XVI. Multi-Session: Power Mgmt Menu will be available for all sessions sharing the access to the serial port with merged outlets for authorized users.

XVII. Events (Syslog messages and/or SNMP Traps): New events for PM PDU and for power supply fails in dual power supply units. The new CYCLADES-ACS5000-TRAP-MIB.ASN file describes the new events.

==========

Fixes

==========

Cyclades ACS 5000 3.3.0-6 release contains the following fixes:

1. LDAPS does not require manual configuration in the /etc/ldap.conf file.
2. The DEFAULT polling rate was changed from 10 to 20 seconds. Data monitoring in this release collects more data than the old version.
3. New MIBs files: CYCLADES-ACS5000-MIB.ASN and CYCLADES-ACS5000-TRAP-MIB.ASN.
4. Deleting SNMP entries via CLI will delete all entries that match the community name (SAP 65610241).
5. Removed the history of logged users due the available space in the RAM disk (SAP 65617136).
6. SNMPD will answer requests for CPU usage without any problem (SAP 65613765).
7. OBWI will redirect to login page received requests without valid authentication (CVE-2011-1037 Access to pages without authentication (Failure to Restrict URL Access)).

==========

Known Issues / Restrictions

==========

Known issues present in this release:

1. Power management is taking longer to get all the information from the PM PDU during start up time when there are a large number of PM PDU units to be detected. During this phase, users can feel some slowness to access the appliance.
2. Configuration of alarm current threshold per segment is not available for Cyclades Intelligent Power Distribution Unit with 2-segment running firmware version 1.8.0 or early
3. Detection of Cyclades IPDU with 2-segment will fail if the unit is daisy chained after an Avocent™ PM PDU running version 1.3.0. This problem affects the Power Device Add operation through DSView™ 3 management software, because the chain will not be detected.
4. Detection of Cyclades IPDU with 2-segment running firmware version 1.9.1 will fail if the unit is daisy chained after a Cyclades IPDU running firmware version 1.9.2.
5. The configuration of polling rate is by IPDU; however it is effective for the serial port. If the serial port has a chain of IPDU units, the poll rate will be the lesser value. The poll rate needs to be greater than the DEFAULT value (20000 ms), if not; the DEFAULT value will be used.
6. The support for '-F' option (force upgrade for the PDU without logical connection) was removed from pmfwupgrade command.
7. Using the Cyclades ACS 5000 console server Web interface, whenever a new user is configured with privileges to manage the outlets of a certain server (Ports -> Physical Ports -> Modify Selected Ports -> Power Management), it is necessary to press buttons "Try Changes" or "Apply Changes" before the new user can be seen in Applications (Applications -> PMD Configuration -> Users Management).
8. The upgrade of the Cyclades ACS 5000 console server firmware code may fail if the internal files are concurrently being accessed by another process or operation. If this occurs, please try firmware upgrading again until it succeeds. When the upgrade operation is performed from DSView 3 software, make sure to review the Operation Results and confirm it has finished successfully before the Cyclades ACS 5000 console server can be rebooted. It is also recommended that the DSView 3 software status polling is disabled while firmware upgrade is run.
   NOTE: Please do not reboot the Cyclades ACS 5000 console server if the firmware upgrade operation has failed. It will render the console server completely inoperable and require technical assistance.
9. The Cyclades ACS 5000 console server Boot Application will **not** be upgraded to support IPV6 protocol, which means that the Cyclades ACS

5000 console server boot configuration will **not** support IPV6 protocol. If firmware upgrade using IPv6 is necessary, the user can do it through FTP or scp using either WMI (Web Management Interface) or CLI (Command Line Interface).

10. IPv6 support will **not** be available for the following services:
    a. IPMI (Intelligent Power Management Interface)
    b. NIS Remote Authentication
    c. Port Virtualization (Clustering)
    d. NFS (Network File System)
    e. LPD (Line Printer Daemon)
11. Samba – client access to the File System with the Microsoft Windows® interface removed from the Cyclades ACS 5000 image due to size limitations.
12. When the Hostname Discovery feature is enabled, the “Physical Ports” screen doesn’t automatically reflect Hostname changes in the servers connected to the Cyclades ACS 5000 console server serial ports. It is necessary to log-out from the web interface, and then log-in again to refresh the browser cache and load the new names.
13. As DHCPv6 protocol does not provide IPv6 prefix lengths, just IPv6 addresses, there must be an IPv6 router providing advertisement messages with network prefixes to the ACS console server when it is configured to obtain its IPv6 address from a DHCPv6 server. If the prefix is not sent by a router, the ACS console server will become unreachable. This is a limitation of the DHCPv6 protocol.
14. When the IPv6 configuration method for the Ethernet interface is set to DHCP, DHCPv6 parameters (stateful IPv6 address, DNS server and Domain name) are accepted even if the "Managed address configuration" and "Other configuration" flags sent by the IPv6 router are not set.
15. If the authentication method is NIS, the user is advised to create an entry for user id 0 in the authentication server; otherwise many of the Cyclades ACS 5000 console server applications may not work. Another option is to always use NIS/Local instead of NIS.
16. Some events that occur in the Windows® operating system environment may not be correctly formatted. For further information go to: *http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/Usage/Windows.aspx*

==========

Configuration Details

==========

Please note the following Configuration Details for this release:

1. It is necessary to configure Hardware flow control in the serial ports configured as dial-in profile (PPP not-auth or PPP) because most of external modem has this configuration by default.
2. It is necessary to explicitly specify the local and remote IPv6 addresses when using PPP connections with IPv6, otherwise the PPP connection will not work (see your installation, administrator and user manual for configuration details).
3. When adding an IPv4 community (SNMP Configuration) and the network is using dual-stack mode, you should configure as source an IPv4-mapped-Ipv6 address.
4. When editing file /etc/resolv.conf manually, there should be no spaces after the addresses configured for DNS servers.
5. It is necessary to edit the /etc/ssl_version.conf file to configure SSL version and cipher level. Follow the syntax:

   SSLVER=<SSLv>

   SSLCIPHER=<level>

   Where:

   <SSLv> - SSL version:

   .. SSLv2 – only version 2

   .. SSLv3 – only version 3

   .. SSLv23 – both version 2 and version 3

   <level> - level of the ciphers:

   .. DEFAULT

   .. HIGH

   .. MEDIUM

   .. LOW

6. When configuring X.509 Authentication in ssh server, the file /etc/ssh/authorized_keys must allow read and write permissions. This can be done by issuing the commands below:

   chmod 600 /etc/ssh/authorized_keys
   chmod 755 /
   config runconfig
   config savetoflash

7. The ‘Hostname Discovery’ feature
   It requires the following configuration in the serial port:
   a) Connection Protocol: Console (Telnet), Console(SSH) or Console(SSH/Telnet)
   b) DCD State: Regard
   c) Data Buffering: Enabled

d) Data Buffering Destination: Local
e) Data Buffering File Size (bytes): 100 or more
f) Hostname Discovery: checked
g) Timeout(seconds): 10

It has by factory default the following configuration:
a) Probe String: “\n”
b) Answer String: "([A-Za-z0-9\._-]+)[ ]+[Ll]ogin[:]?[ ]?$"
   This answer will match most of Unix

It uses the following regular expression in Answer String to match the hostname: ([A-Za-z0-9\._-]+).
Examples of Answer String:
a) Most of Linux machines, the hostname comes in the login prompt, for example “MY-Linux login:”
   The answer string "([A-Za-z0-9\._-]+)[ ]+[Ll]ogin[:]?[ ]?$" will get MY-Linux as the hostname of the server.
b) Cisco routers, the hostname comes in the prompt, for example “Cisco2522>”.
   The answer string “([A-Za-z0-9\._-]+)[>#]” will get the Cisco2522 as the hostname of the device
c) ACS 6000 appliance, the hostname comes in the middle of the banner, for example “ACS6000 2.0.1.3-20090507 MY-ACS6048 ttyS0”
   The answer string “ACS6000 [^]* ([A-Za-z0-9\._-]+) ttyS” will get the MY-ACS6048 as the hostname of the ACS 6000.