aaa-reports! white paper

Enhanced Reporting & Audit Compliance
For
TACACS+ Device Administration
Via
Cisco Secure ACS

Contents

Terminology

ACS	Cisco Secure ACS
ACS UI	CSAdmin web based management user interface for ACS
COBIT	A set of best practices for the management of IT systems
DCS	Device Command Set. A set of TACACS+ device command authorisations shared by ACS Groups and Users. AKA “Command Set”
NAR	Network Access Restriction. A set of rules for filtering which devices (or NDGs) can be accessed. NARs can be defined within an ACS Group/User or as an SPC
NDG	Network Device Group. A collection of AAA Client devices.
SPC	Shared Profile Component. A feature in ACS whereby re-usable named “chunks” of configuration can be defined and referenced elsewhere. ACS provides SPCs for NARs and DCS amongst others.
TDA	TACACS+ Device Administration. A feature whereby network device administration is authorised via the TACACS+ protocol by ACS.
SOX	Sarbanes Oxley auditing requirements

Background

TDA as an ACS feature evolved over time with each new feature set augmenting (rather than replacing) the previous one. This has resulted in some confusion because what appears to be the same function may have several names in ACS.

TDA breaks down into three main areas in ACS:

- **Network Access Restrictions**. NARs control which devices a member of an ACS group may logon to. Originally NARs were all group level, but in ACS v3.x Shared NARs allowed named NARs to be defined once and re-used in many groups.
- **Service Authorisation**. Before admin's can do anything they need to establish a session on the device in question. The ACS service authorisation (shell, pixshell etc) define whether this is allowed and also provision the access device with session parameters (eg idle timeout)
- **Command Authorisation**. Assuming a session is established on the device, command authorisation is then used to control what actions the administrator can perform.

There are three distinct types of Command Authorisation used by most customers:

- **Enable Authorisation**. The "old way".. on each and every device commands are configured to require a specific permission level (0..15). After logging into the device the admin user performs a second "enable authentication" which results in ACS giving back the permission level. This level is then applied to any commands issued on the device[1].
- **Group Level Command Authorisation**. This offers a finer degree of control by configuring a list of permitted/denied commands statically within each ACS group. However, the authorisations are applied the same regardless of which device group the administrator is working on. Also it doesn't scale well as the same data may have to be entered for multiple ACS groups – which is both time consuming and error prone.
- **DCS Authorisation**. The "final solution"… command authorisation data is defined in re-usable shared profiles via ACSs SPC architecture. Within each ACS group a mapping from NDG to DCS allows for the definition of "roles". Ie a group becomes a role where any given role may require differing permissions based on the device being managed.

[1] Note that when NDG→DCS mappings were implemented, the enable feature was also updated to include NDG→Priv Level mapping also.

SOX & COBIT

From an IT security perspective, SOX is vague in many areas, especially as it relates to the specifics of, "how to comply" because SOX does not provide exact security procedures or processes that companies will need to have in place for compliance. Nor does it recommend any specific IT solution for compliance. On the other hand, there are parts that are very specific and have a direct impact on IT budgets. For example, the law states that all business records, including electronic records and electronic messages, must be saved for "not less than five years." With this data-storage requirement it is clear that SOX has and will continue to have a noticeable effect on corporate IT departments.

In addition to the obvious and "between the lines" IT requirements, SOX mandates corporations to demonstrate sound financial controls governing their business processes and then test those controls quarterly. Of course, manually documenting and testing these controls is one way to do that, but the costs for labour and time would be considerable and present a procedural and logistical nightmare. It just makes sense that companies would look to automate as much of the process with software and hardware platforms to quickly address their dilemma.

COBIT has been designed to in part to provide IT decision makers with the information they require to assess not only new but currently deployed systems also. At the core of the many activities lays monitoring and reporting, with the documentation and operational audit of Control Practices being of particular interest to the network administrator. At very least there should be documentation that clearly defines the control practices in use and regular audits to show how effective these practices are when deployed.

A typical AAA server such as Cisco Secure ACS may contain three primary network security policies:

- Network end-user/identity access control (VPN, Wifi, VLAN etc)
- Network administrator user access control (typically TACACS+ Device Administration)
- AAA Server administrator access control (ie config changes on the AAA server itself)

In addition to the raw policy data "locked up" inside the ACS database the mass of accounting, authentication, administration event and failure logs hold a wealth of valuable data. From the viewpoint of good governance it is critical to be able to:

- Validate the policies in place are actually working with no unforeseen consequences
- Easily spot exceptions and violations of policy
- Instigate a forensic analysis of the logs to find out what really happened.

aaa-reports! Reports Available

Reports fall roughly into three categories:

- **Policy Documentation**. These are designed simply to document the policies as configured. Without aaa-reports! many customers resort to printing screen dumps of the ACS UI. There are reports to document:

    - Group/User feature usage summary list (ie a tick for each each TDA feature[2] used)
    - Group/User policy details (details of configured elements such as NAR, Enable etc)
    - Shared NAR/DCS summary (list of groups with the NARs/DCSs they reference)
    - Shared NAR/DCS details (detailed list of NAR/DCS content)
    - Shared NAR/DCS references. Lists the groups that make an active (ie enabled) reference to a named NAR or DCS. Useful for change impact analysis
    - Unreferenced NAR/DCS. Lists any that do not have an active reference and are therefore possibly redundant
    - Network Device Group details (list of devices making up each NDG)

- **Policy Evaluation**. These are designed to evaluate the policies in order to provide answers that might otherwise require hours of pouring over the documentation reports.

    - Authorised devices. Lists the devices (or device groups) that a user or group specifically can or cant access (via NARs)
    - Authorised Commands. Lists the commands that a user or group may (or may not) execute against devices (via NDG → DCS mappings)
    - Is a device permitted? For a named device this report will show those groups who specifically have permit access.

- **Current User Status**. These provide information as to the current state of individual user accounts within the database wrt account expiry, password aging status etc.

[2] TDA features include: Shell/PixShell Service, IP Based NARs, Enable Authorisation & Command Authorisation

Using the Reports

Exporting the ACS Policy Information

Before any of the TDA reports can be run the ACS user/group database has to be exported and copied onto the server running aaa-reports! Depending on the version and type of ACS server (software or appliance) this can be more (or less) challenging. The table below shows the various supported routes:

ACS Version	ACS Type	Supported	Method
3.x	Appliance	No	
3.x	Software	Yes	GetAcsDb script*
4.x	Appliance	Yes	CSAdmin support cab file**
4.x	Software	Yes	CSSupport cab file***

* The script GetAcsDb is installed as part of aaa-reports! and can be copied onto the server hosting ACS. It comprises a .bat and .vbs file and requires the latest version of Windows Scripting Host to be present. This script attempts to harvest both the user/group and network configuration databases into a single .cab file.

** On the appliance support web page there is an option to generate a support cab file and download over FTP. The option to include the User/Group database should be ticked.

*** In the ACS bin folder the CSSupport.exe can be used to generate a cab file. Make sure both the User/Group database and Registry components are selected. Logs are not required.

Note that all of the above methods of exporting data will result in a brief interruption to the ACS service. Care should be taken when choosing the time to perform this task to avoid user connection problems.

Importing into aaa-reports!

Once the ACS database has been harvested and copied onto the server hosting aaa-reports! it's a simple task to import. On the "Import" page click "Import ACS Database" and follow the on-screen instructions where you will be prompted for the location of your cab file. Aaa-reports! will open the cab file, extract the user/group & network config databases and then import them.

Note that occasionally ACS cab files can be corrupted (either at time of generation or during the file copy) and become unreadable by aaa-reports! If this occurs a cab repair tool can be used to fix the corruption, or easier still, a utility such as Winzip can be used to extract the contents. If aaa-reports! cannot open the cab file it will prompt you for a location holding the unpacked contents.

Running the reports

Once the ACS database has been successfully imported, the reports on the "ACS/TDA Policy" tab of the "Reports" page can be run just like any other standard canned report with one exception. Many of the reports take parameters that can be wildcards such as * to allow multiple groups, users, DCS or NARs to be included in the report.

TDA Group Summary Report

This report lists of any groups that have a TDA related setting configured. This report provides an "at a glance" view of the groups that are of interest. Only those groups with at least one TDA related setting are included.

Note that this report does not attempt to report what the configuration settings are, only that they exist.

TDA Group Summary *aaa-reports!*

Group	Users	Group NARs	Shared NARs	Enable	Shell/Exec	Shell Cmd Authorisation	PixShell	Pixshell Cmd Authorisation
96 : Enable Test	0			Yes				
97 : Contractors	1	Yes						
98 : LAN Admins Audit	1		Yes		Yes	Yes		
99 : LAN Admin Super	2		Yes	Yes	Yes	Yes		
100 : LAN Admins West Coast	2		Yes		Yes	Yes		
101 : LAN Admins East Coast	2		Yes		Yes	Yes		
102 : LAN Admins EMEA	2		Yes		Yes	Yes		
103 : LAN Admins ASIAPAC	2		Yes		Yes	Yes		

TDA User Overrides Summary Report

Similar to the group summary, but for users. This report shows those users with settings that override the group policy, ie having TDA features configured with a setting other than "as per group".

Ideally users should obtain authorisations as a result of their group membership and role (ie NDG→DCS mapping) and user specific settings should not be required. However in the "real world" there will always be corner cases as displayed in this report.

TDA User Summary aaa-reports!

Username	Group	User NARs	Shared NARs	Enable	Shell/Exec	Shell Cmd Auth	PixShell	Pix Cmd Auth
bilbo	97 : Contractors	Yes		Yes				
boromir	102 : LAN Admins EMEA			Yes				
daz	0 : Default Group			Yes				
elrond	98 : LAN Admins Audit			Yes				
Faramir	102 : LAN Admins EMEA			Yes				
gandalf	99 : LAN Admin Super			Yes				
gimli	103 : LAN Admins ASIAPAC			Yes				
legolas	103 : LAN Admins ASIAPAC			Yes				
Saruman	99 : LAN Admin Super		Yes		Yes	Yes		

TDA Group Shared NAR/DCS Summary Report

This report provides an "at a glance" view of each ACS group that has either Shared NARs or DCSs and as such give a summary of the ACS groups, the devices they can administer and the command authorisations applicable.

TDA Group Shared NAR/DCS Summary aaa-reports!

Group	Users	Shared NARs	Shell Cmd Set	Pixshell Cmd Set
98: LAN Admins Audit	1	AccessAll	NoAuthorisation ReadOnly	
99: LAN Admin Super	2	AccessAll	SuperUser	
100: LAN Admins West Coast	2	AccessEastCoast AccessWestCoast	LanManagement NoAuthorisation ReadOnly	
101: LAN Admins East Coast	2	AccessEastCoast AccessWestCoast	LanManagement NoAuthorisation ReadOnly	
102: LAN Admins EMEA	2	AccessASIAPAC AccessEMEA	LanManagement NoAuthorisation ReadOnly	
103: LAN Admins ASIAPAC	2	AccessASIAPAC AccessEMEA	LanManagement NoAuthorisation ReadOnly	

Note that there is no relationship between the data in the Shared NARs column and Shared DCS. Each simply lists the items referenced within each group.

TDA User Shared NAR/DCS Summary Report

This report is essentially the same as TDA group NAR/DCS report but for users.

Shared NARs Summary

This report shows a summary of every Shared NAR and the AAA Clients they control access to (either permit or deny).

TDA Shared NARs Summary aaa-reports!

Name	Description	Type	Permit/Deny	AAA Clients
AccessAll	Allow Access to all regions	IP Based	Permit	*

Name	Description	Type	Permit/Deny	AAA Clients
AccessAllExceptASIAPAC	Allow Access to all except ASIAPAC	IP Based	Deny	NDG:ASIAPAC

Name	Description	Type	Permit/Deny	AAA Clients
AccessASIAPAC	Allow Access to ASIAPAC	IP Based	Permit	NDG:ASIAPAC

Name	Description	Type	Permit/Deny	AAA Clients
AccessEastCoast	Allow Access to East Coast	IP Based	Permit	NDG:East Coast US

Name	Description	Type	Permit/Deny	AAA Clients
AccessEMEA	Allow Access to EMEA	IP Based	Permit	NDG:EMEA

Name	Description	Type	Permit/Deny	AAA Clients
AccessWestCoast	Allow Access to West Coast	IP Based	Permit	NDG:West Coast US

Note that the "AAA Client" values are as entered into the ACS configuration.. they can contain individual device names, NDG or NAF names.

Shared NARs Details

This report lists of the selected Shared NARs and gives detailed content. This report could be run against a specific NAR or all NARs.

TDA Shared NARs Details for: Access* aaa-reports!

Name AccessAll
Description Allow Access to all regions
Type IP Based
Defines Permit

AAA Client	Port	Address:
NDG:West Coast US	*	*
NDG:East Coast US	*	*
NDG:EMEA	*	*
NDG:ASIAPAC	*	*

Shared DCS Summary

This summary report lists each Device Command Set and a basic list of commands that it contains.

TDA Shared DCS Summary (Shell/Exec) aaa-reports!

Name	Description	Unmatched Cmds	Commands
AnotherDCS	Just another example	deny	
LanManagement	Switch port config	deny	switchport speed show set no interface duplex description configure

Shared DCS Details

This report shows full detail for one or more DCSs.

TDA Shared DCS Details (Shell) for: *

Name LanManagement
Description: Switch port config
Unmatched Commands deny

Command	Unmatched Arguments	Argument
configure	deny	permit terminal
description	permit	
duplex	permit	
interface	permit	
no	permit	permit shutdown
set	permit	permit "port enable" permit "port description" permit "port speed" permit "port host" permit vlan permit "port duplex"
show	deny	
speed	deny	
switchport	deny	permit host permit access permit "mode access"

Enable Details Report

This report lists any groups that have Enable Authorisation configured together with the actual privilege levels (or mappings based on NDG)

TDA Enable Details aaa-reports!

Group Name	Type:	Max Priv	NDG	Priv Level
96 : Enable Test	Per NDG		West Coast US	1
			ASIAPAC	15
			EMEA	15
			East Coast US	1
99 : LAN Admin Super	All AAA Clients	15		

TDA Group Detail

For the purposes of documenting the group policy this report closely resembles the ACS group edit UI page. The report will look slightly different depending on what TDA features are enabled and how they are configured, however the example below is representative.

TDA Group Detail: LAN Admins East Coast aaa-reports!

Access Restrictions

Shared NARs	Enabled	
	Allow access when	All NARs must result in permit
	Selected NARs	AccessEastCoast AccessWestCoast
Group IP-Based NARs	Disabled	

Enable Authorisation

Enable Authorisation	Disabled

Shell (Exec) Service Authorisation

Shell (Exec) Service	Enabled		
	Service Attributes	Name	Value
		timeout	60
		priv-lvl	15
		idletime	60
Shell Cmd Authorisation	Enabled		
	DCS per NDG	NDG Name	DCS Name
		East Coast US	LanManagement
		West Coast US	ReadOnly
		<DEFAULT>	NoAuthorisation

Pixshell Service Authorisation

PIX Shell Service	Disabled
PIX Shell Cmd Authorisation	Disabled

TDA User Detail

This report has the same format as the TDA Group Detail report and is used to document those users who have settings that override group policy. It will only include those features configured with a value other than "as per group".

TDA User Detail: Saruman

aaa-reports!

ACS Group	000 : Default Group		
Access Restrictions			
Shared NARs	Enabled		
	Allow access when	All NARs must result in permit	
	Selected NARs	AccessAllExceptASIAPAC	
User IP-Based NARs	As Per Group		
Enable Authorisation			
Enable Authorisation	As Per Group		
Shell (Exec) Service Authorisation			
Shell (Exec) Service	Enabled		
	Service Attributes	Name	Value
		timeout	30
Shell Cmd Authorisation	Enabled		
	DCS per NDG	NDG Name	DCS Name
		<DEFAULT>	ReadOnly
Pixshell Service Authorisation			
PIX Shell Service	As Per Group		
PIX Shell Cmd Authorisation	As Per Group		

Group Authorised Devices (NAR) Report

The key question asked during a security audit is "Which devices can users of a group gain access to?"… and conversely any devices that are specifically not allowed.

For a given group, this report lists the devices (or device groups) that can (or can't) be accessed. This involves looking at the group to decide what if any NARs are active (group level or shared).

Note that where the NAR type is deny, this is actually permitting access to ALL devices EXCEPT those listed. However, for clarity the report will simply give the access type as either permit or deny.

The examples below are for two different groups:

TDA Group Authorised Devices (NAR) for LAN*

aaa-reports!

Group 100 : LAN Admins West Coast

Access Type	AAA Client	via NAR
Permit	NDG:East Coast US	AccessEastCoast
Permit	NDG:West Coast US	AccessWestCoast

TDA Group Authorised Devices (NAR) for LAN*

aaa-reports!

Group 98 : LAN Admins Audit

Access Type	AAA Client	via NAR
Permit	NDG:ASIAPAC	AccessAll
	NDG:West Coast US	
	NDG:EMEA	
	NDG:East Coast US	

Note that where group level NARs are used the "via NAR" column would simply contain the value "Group Level"

User Authorised Devices (NAR) Report

This report is the same as Group Authorised Devices report, but for. This report can be used in conjunction with the group level version to show the complete authorisation for a user. It does not attempt to perform the ACS policy "merging" performed between group and user level NARs.

Note that for users without any specific configuration, the data is picked up from that users group and therefore will look identical to the group level report.

Group Authorised Commands (DCS) Report

Being able to know what devices can be accessed is only half the story and so the follow-on question is "What commands can users of a group execute, and on which devices?"

This report shows the command authorisations for each NDG configured for one or more groups. Note that it does not include "group level command authorisation" because by definition such a configuration is applied equally to all devices and so the Group Detail report should be used.

TDA Group Authorised Commands (Shell) for: LAN Admins EMEA aaa-reports!

Group 102 : LAN Admins EMEA

NDG(s)	DCS	Unmatched Cmds	Cmd	Unmatched Args	Args
EMEA					
	LanManagement	deny	set description	permit	vlan
			duplex		
			interface		
			no	permit	shutdown
			set	permit	"port description"
			set	permit	"port duplex"
			set	permit	"port enable"
			configure	permit	terminal
			set	permit	"port speed"
			show		
			speed		
			switchport	permit	"mode access"
			switchport	permit	access
			switchport	permit	host
			set	permit	"port host"
<DEFAULT>					
	NoAuthorisation	deny			
ASIAPAC					
	ReadOnly	deny	show	permit	all
			ping		

In the example above the group "LAN Admins EMEA" may access the EMEA and ASIAPAC device groups but with different authorisations on each.

User Authorised Commands (DCS) Report

This report is the same as the Group Authorised Commands (RCS) report, but for users. If the user has no data configured (or set to "as per group") the settings are picked up from the group to which the user is a member.

Unreferenced NAR/DCS Report

A question that often arises during day-to-day management of an ACS server it “How do I check that all of the NARs and DCSs are needed? Ie are any just sitting there not being referenced at all?”

The unreferenced NAR/DCS report lists an NARs or DCSs that have no references and can are therefore redundant in the currently active security policy. This could be by design or because of a mis-configuration.

TDA Unreferenced NAR/DCS aaa-reports!

DCS

Name
AnotherDCS

NAR

Name
AccessAllExceptASIAPAC

Shared DCS Reference/Usage Report

Before making a configuration change it is critical to know what groups/users will be effected – before you make it. This report shows the groups that use any given DCS plus (if TACACS+ Administration logs are imported) the last date on which the DCS caused an authorisation failure.

For each (or specific) DCS show the groups (& associated NDG mappings) and any users that make reference to it. The report will tell the customer which groups/users are referencing the DCS and for what group of devices. Also whether (and how much) the configs are actually being used.

Note that only users with specifically assigned DCS are listed in the "User References" sub-section.

TDA Group Shared DCS Reference/Usage for: ReadOnly aaa-reports!

DCS ReadOnly

Group		Users	Network Device Group	Last Denial	Cmd Denies
98	LAN Admins Audit	1	EMEA	30/11/2006	3
100	LAN Admins West Coast	2			
101	LAN Admins East Coast	2			
102	LAN Admins EMEA	2			
103	LAN Admins ASIAPAC	2			

Shared NAR Reference/Usage Report

Similar to the DCS References Report except that with NARs there are no NDG mappings. More importantly for the usage, NAR info only gets logged if a user is filtered as this is the only meaningful metric.

As per the Shared DCS references report, both group and user level references are included.

TDA Group Shared NAR Reference/Usage for: AccessEastCoast *aaa-reports!*

Name: AccessEastCoast

Group		Users	Last Trigger	Authen rejects for last 30 days
101	LAN Admins East Coast	2	30/11/2006	1
100	LAN Admins West Coast	2		