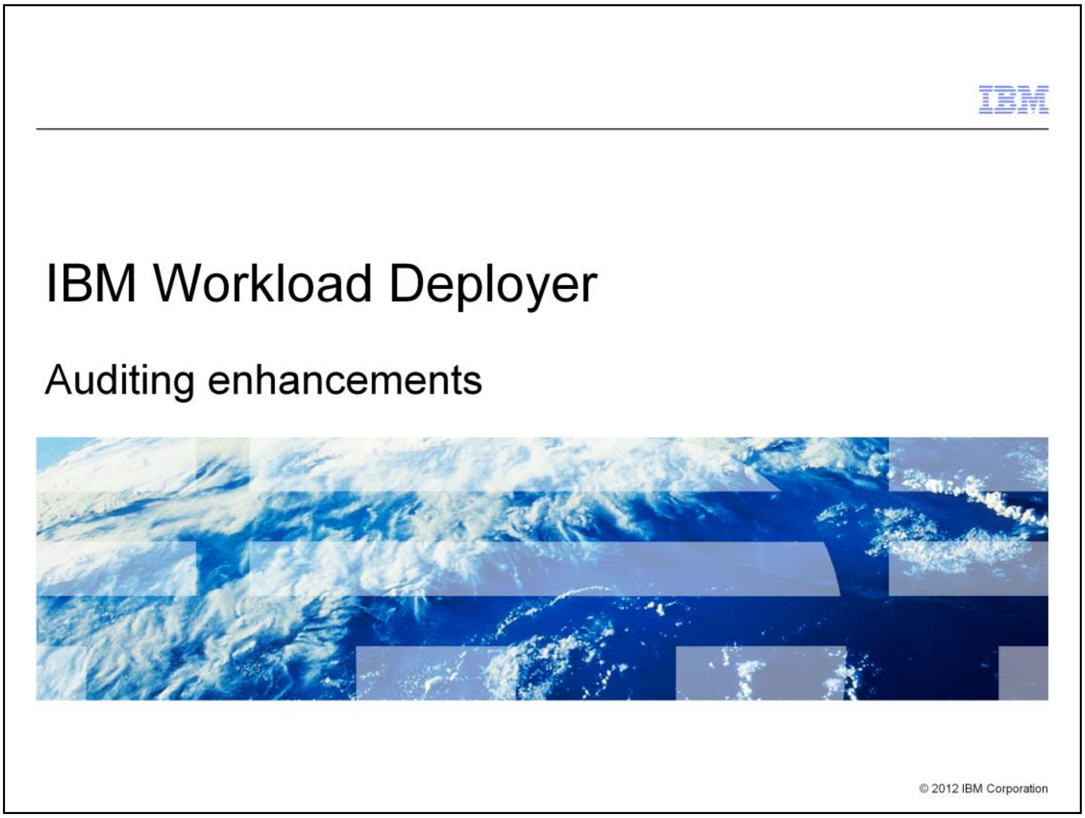
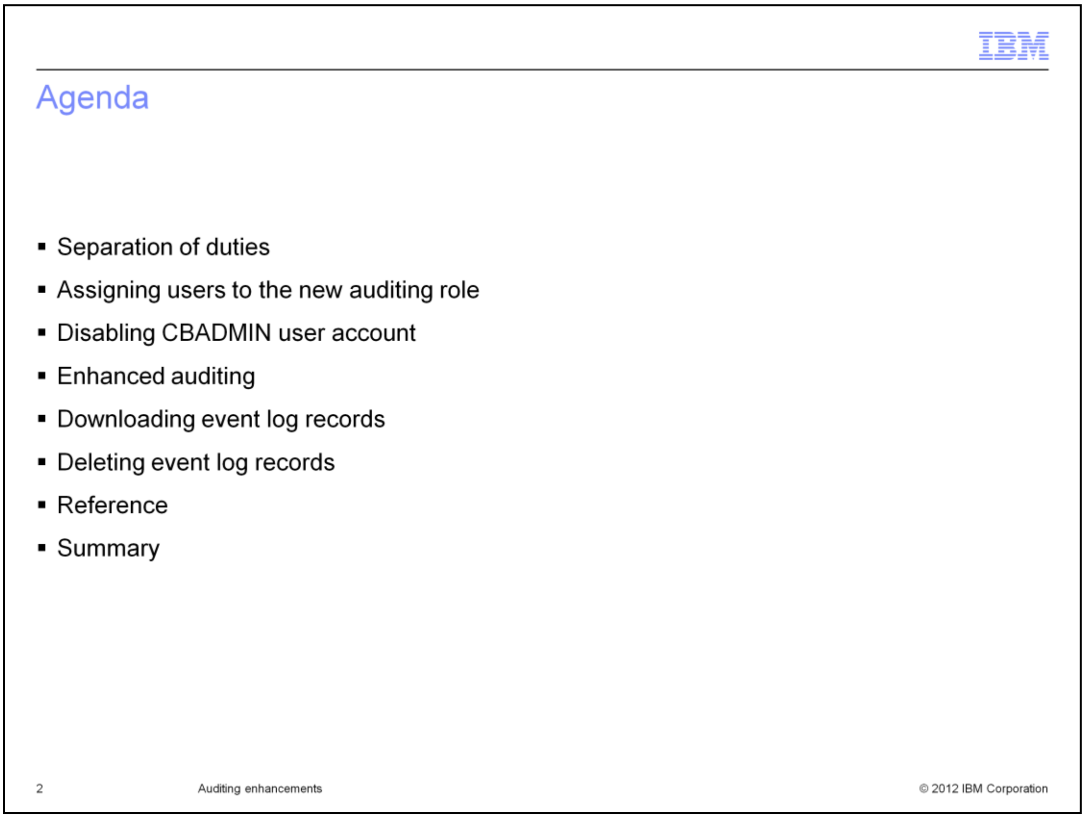


IBM Workload Deployer

Auditing enhancements

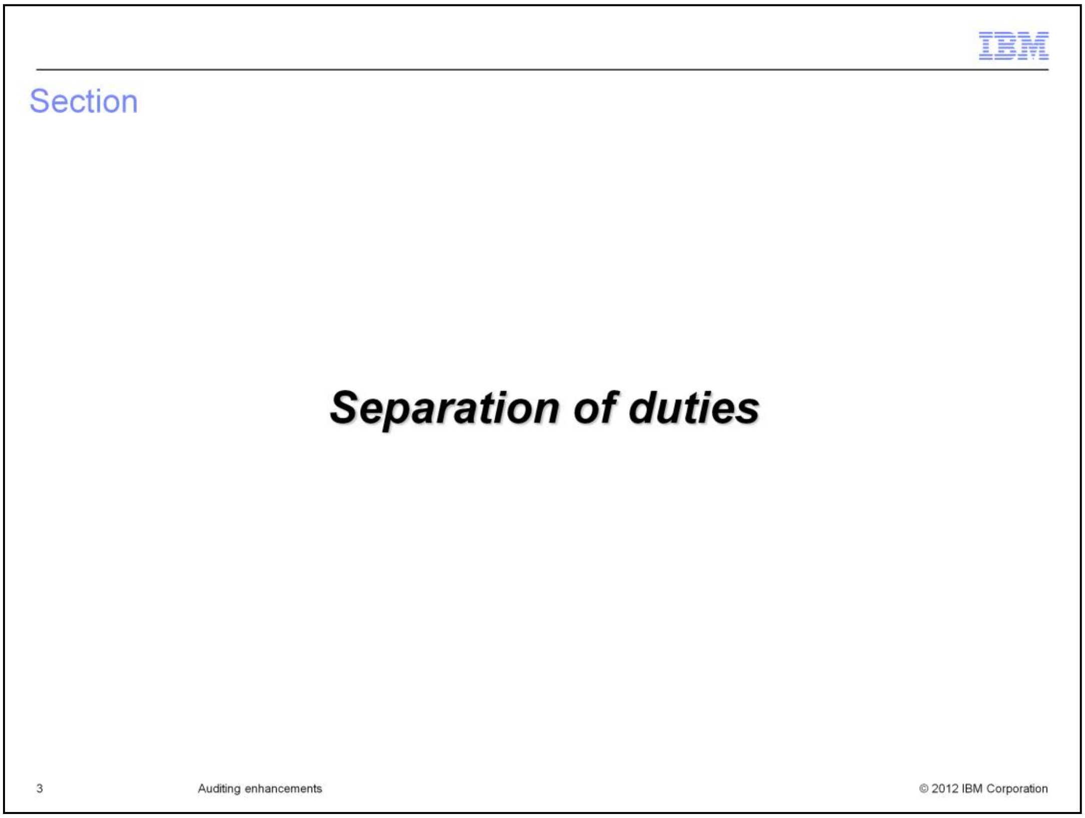
This presentation covers IBM Workload Deployer auditing facility enhancements available with IBM Workload Deployer V3.1.



Agenda

- Separation of duties
- Assigning users to the new auditing role
- Disabling CBADMIN user account
- Enhanced auditing
- Downloading event log records
- Deleting event log records
- Reference
- Summary

This presentation discusses, the separation of the auditing and appliance administration duties. Assigning users to the new auditing role. The disablement and re-enablement of the CBADMIN user account. Enhanced auditing functionality. Downloading event log records. Deleting event log records. Helpful references. And a summary of this presentation.

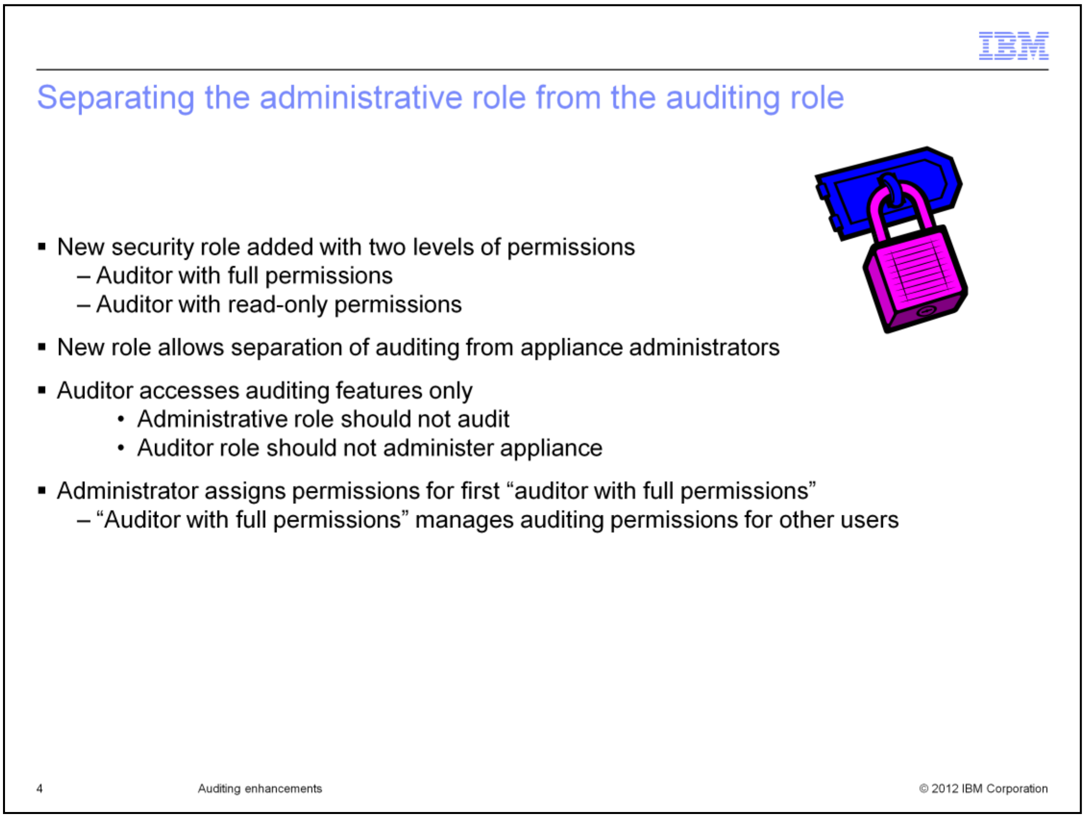


Section

Separation of duties

3 Auditing enhancements

This section discusses the separation of duties and introduces the new auditing role.



Separating the administrative role from the auditing role

- New security role added with two levels of permissions
  - Auditor with full permissions
  - Auditor with read-only permissions
- New role allows separation of auditing from appliance administrators
- Auditor accesses auditing features only
  - Administrative role should not audit
  - Auditor role should not administer appliance
- Administrator assigns permissions for first “auditor with full permissions”
  - “Auditor with full permissions” manages auditing permissions for other users

4 Auditing enhancements © 2012 IBM Corporation

IBM Workload Deployer now requires the formal assignment of an auditor role for working with auditing data. This is designed to separate the duties between an auditor role and an administration role. Administrators should not be able to audit, and auditors should not be able to administer the appliance.

IBM Workload Deployer v3.1 introduced a new auditor role for this purpose. Within the auditor role, there are two levels of permissions - full permissions and read-only permissions.

Further, this separation of duties affects how permissions are granted to other users. The appliance administrator must set the permissions for the first user with “auditor with full permissions”. After that, the “auditor with full permissions” can assign or revoke auditing permissions for other users.

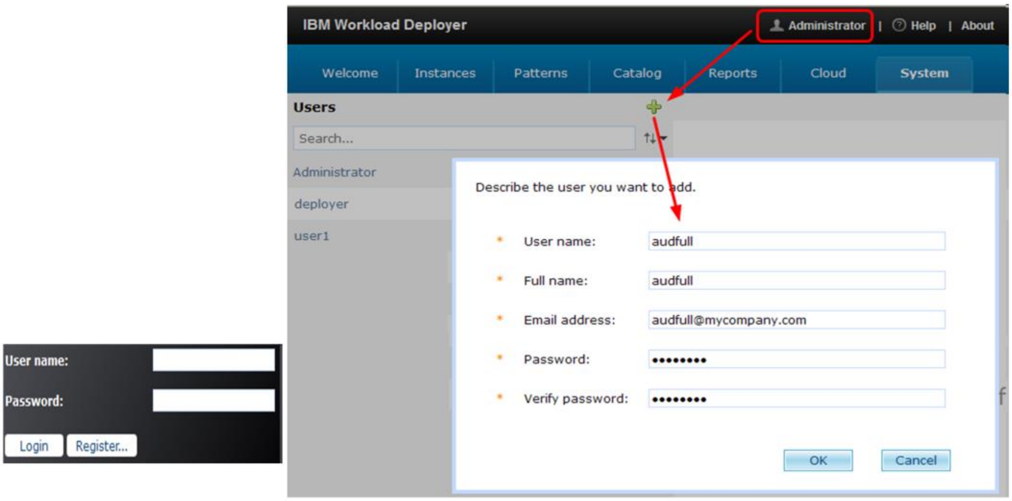
Section

Assigning users to the new auditing role

This section discussing how you assign users to the new auditing role.

Creating users for auditing

- Appliance administrator must create **all** user accounts for the auditor role
- Or, if self-registration is enabled, a potential auditor can register his own user account
- “Deploy patterns in the cloud” permission is default for all user accounts

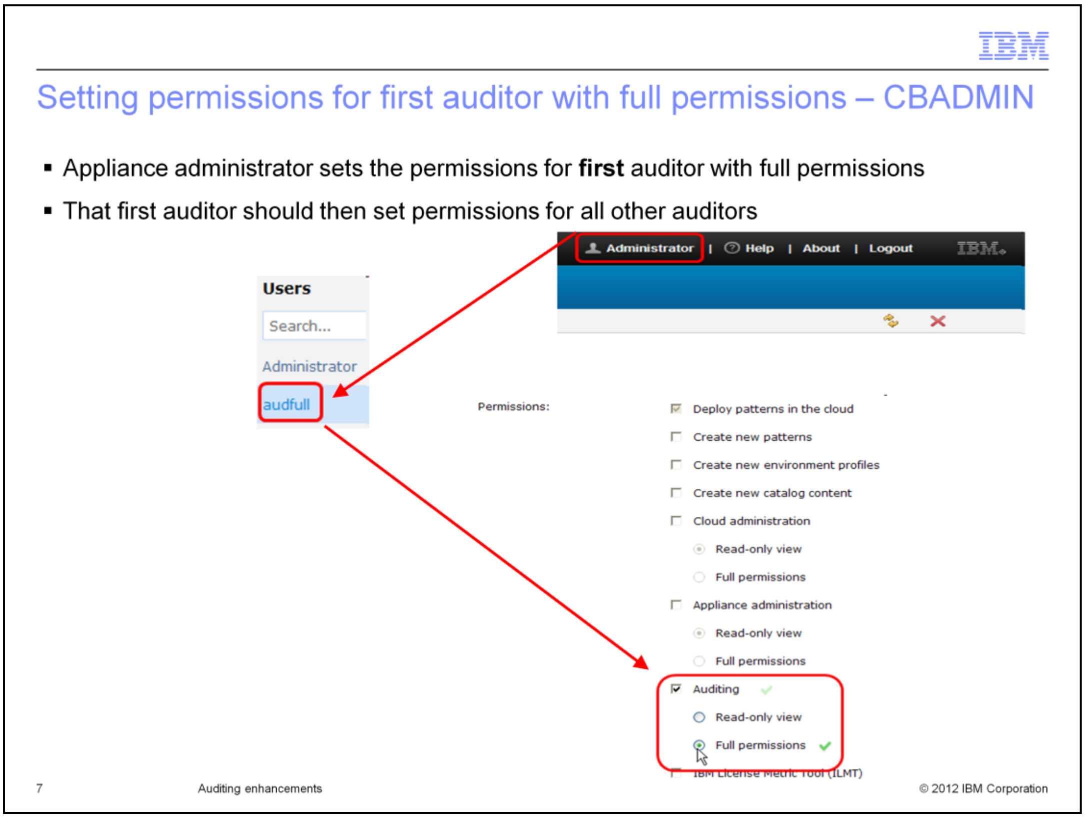


User name:
Password:

Describe the user you want to add.

- User name: audfull
- Full name: audfull
- Email address: audfull@mycompany.com
- Password: ••••••••
- Verify password: ••••••••

User account creation is the same for auditors as for any other user. If it is done using the administrative console, an administrator with full permissions creates the user accounts. The example shows the appliance administrator creating the first user account that is to be given the “auditing with full permissions” role. If self-registration is enabled, then an auditor (or any other user) can register for a user account. In either case, the default permission of “Deploy patterns in the cloud” is a fixed permission given to all user accounts.



Setting permissions for first auditor with full permissions – CBADMIN

- Appliance administrator sets the permissions for **first** auditor with full permissions
- That first auditor should then set permissions for all other auditors

Users

Search...

Administrator

audfull

Permissions:

☑ Deploy patterns in the cloud
☐ Create new patterns
☐ Create new environment profiles
☐ Create new catalog content
☐ Cloud administration
  ● Read-only view
  ○ Full permissions
☐ Appliance administration
  ● Read-only view
  ○ Full permissions
☑ Auditing ✓
  ○ Read-only view
  ● Full permissions ✓
☐ IBM License Metric Tool (ILMT)

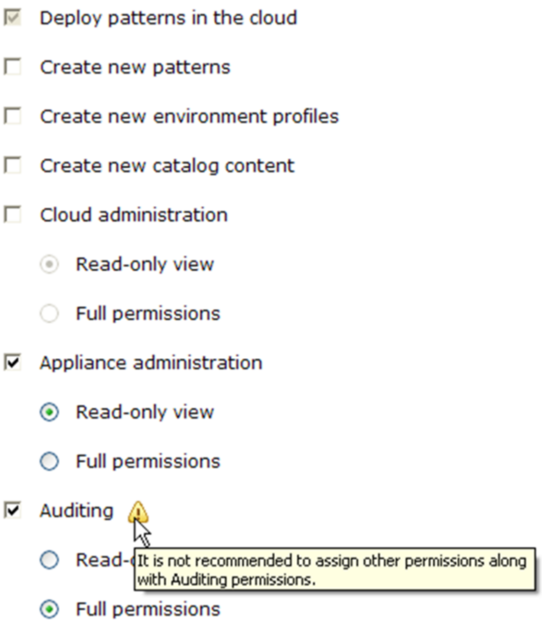
7 Auditing enhancements © 2012 IBM Corporation

As part of the separation of duties, the appliance administrator should set the permissions for the first auditor with full permissions ONLY. It is not recommended, but there is nothing stopping the administrator from setting multiple auditors with either full or read-only permissions. The recommendation is that the first auditor with full permissions manages the setting of permissions of any other user accounts that are potential auditors.

Note that an auditor user cannot reset their own permissions; another auditor - or less desirably the administrator - must reset the auditing permissions.

Warning when mixing roles

- Appliance provides guidance when assigning permissions
- Auditing permissions should not be mixed with other permissions
  - Exception: Deploy patterns in the cloud is assigned to everyone by default



☑ Deploy patterns in the cloud

□ Create new patterns

□ Create new environment profiles

□ Create new catalog content

□ Cloud administration

● Read-only view

○ Full permissions

☑ Appliance administration

● Read-only view

○ Full permissions

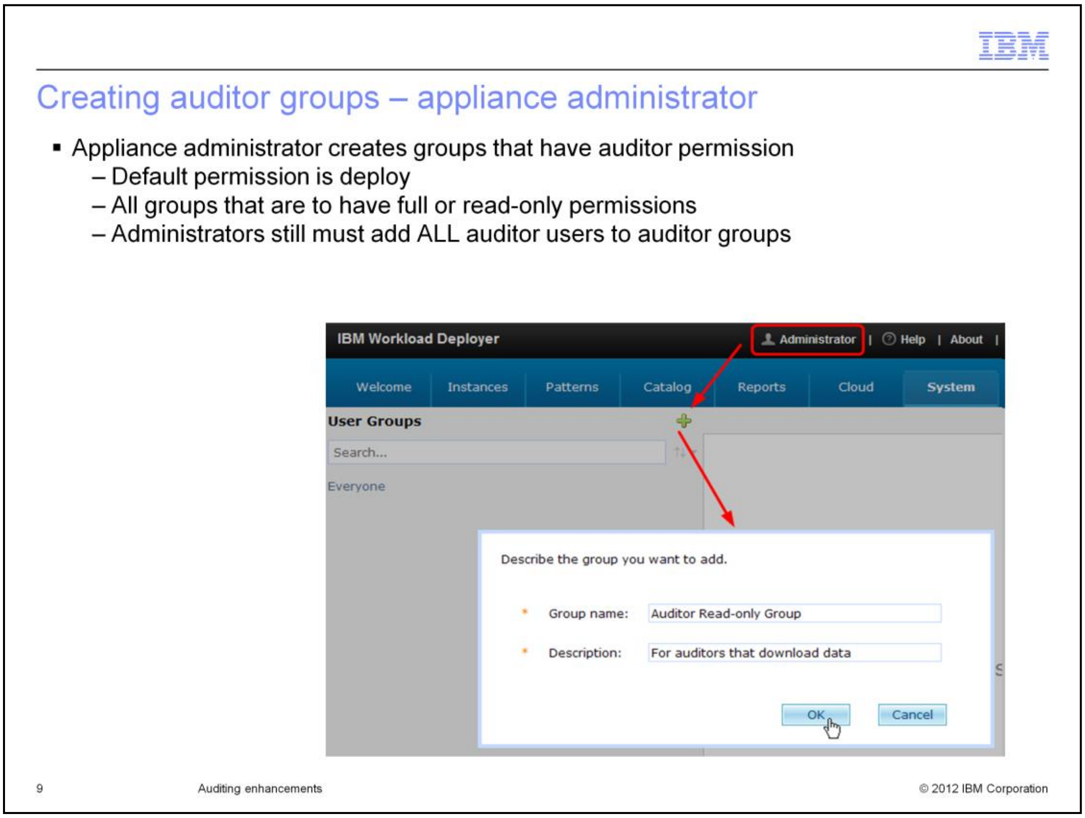
☑ Auditing ⚠

○ Read-

It is not recommended to assign other permissions along with Auditing permissions.

● Full permissions

If a user is given auditing permissions and given any other permissions except the default “Deploy patterns in the cloud” permission, a warning message is displayed indicating that this is not recommended. The example shows the warning message when a user was given “Auditing with full permissions” along with “appliance administration”.



Creating auditor groups – appliance administrator

- Appliance administrator creates groups that have auditor permission
  - Default permission is deploy
  - All groups that are to have full or read-only permissions
  - Administrators still must add ALL auditor users to auditor groups

Describe the group you want to add.

* Group name: Auditor Read-only Group

* Description: For auditors that download data

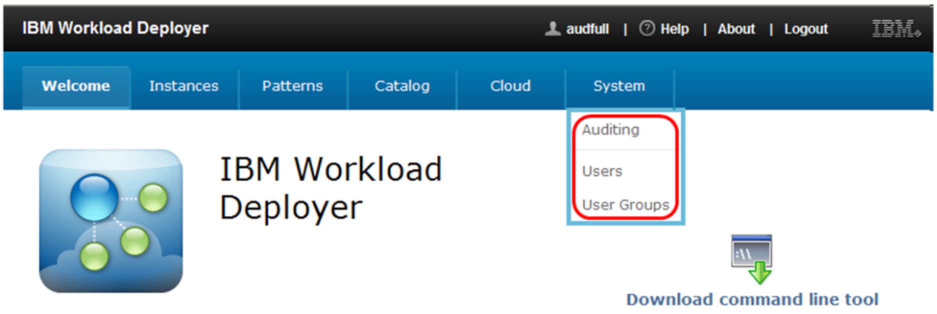
9 Auditing enhancements

Auditor group creation is similar to auditor user creation. All auditor groups must be created by an appliance administrator having full permissions. (There is no self-registration for groups). The group that is to have auditing full or read-only permission is assigned their auditing permission by another auditor that has full permissions. There is nothing stopping an administrator from setting the auditor group permissions, but best practice prescribes that an auditor with full permissions should set the auditing permissions.

Note that only administrators have the permission to add auditor users to auditor groups.

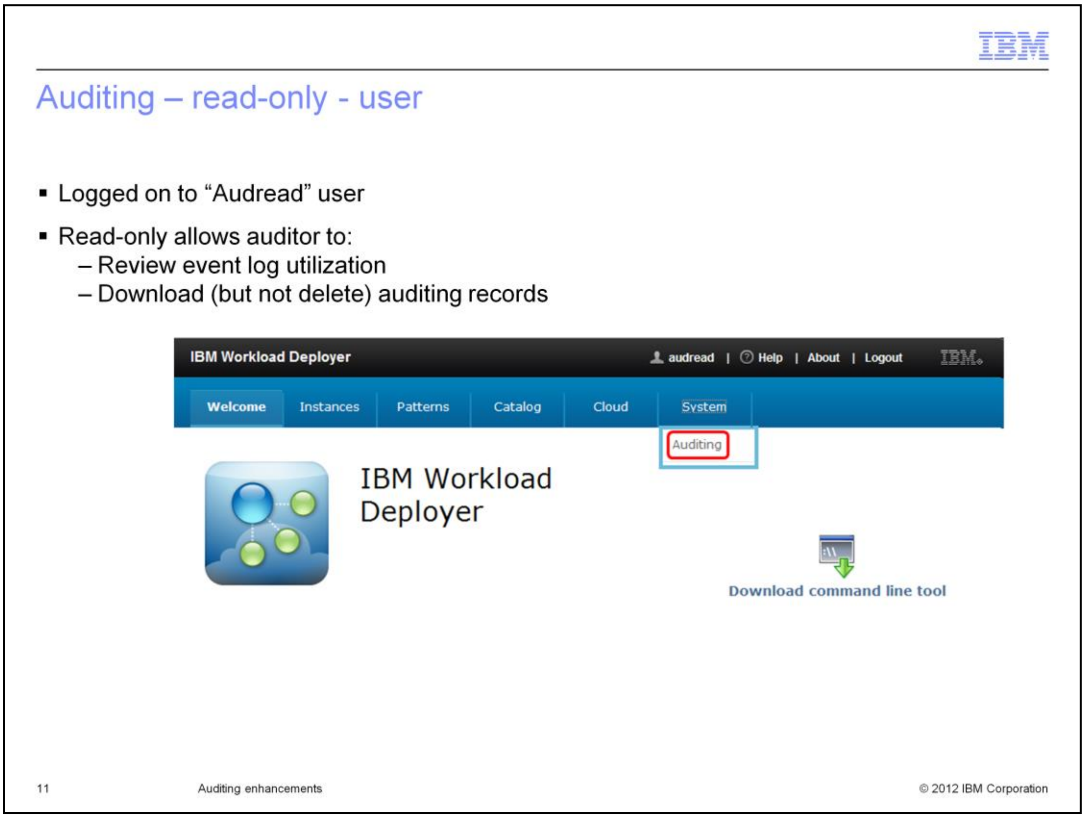
Auditing – full permissions - users

- Logged on to “Audfull” user
- Primary functions
  - Managing auditing permissions in users and groups
    - Allows users with “auditing with full permissions” role to manage the auditing role of other users
  - Review event log utilization
  - Download auditing records
  - Delete auditing records



When you log into IBM Workload Deployer as an auditor with full permissions, the menu dynamically matches your permissions. While an “auditor with full permissions” also has the permission “Deploy patterns in the cloud”, working with cloud resources is not the auditor’s intended role. The primary function of the “auditor with full permissions” is to manage auditing permissions for auditor users and auditor groups, and to work with auditing records. The auditing-related selections are under the System pull-down menu.

From the **Auditing** menu, an auditor can review the event log utilization and download log records. Additionally, by using the REST API interface, an auditor with fill permissions can delete auditing records, which does need to be done on a regular basis as there is limited space for the auditing records.



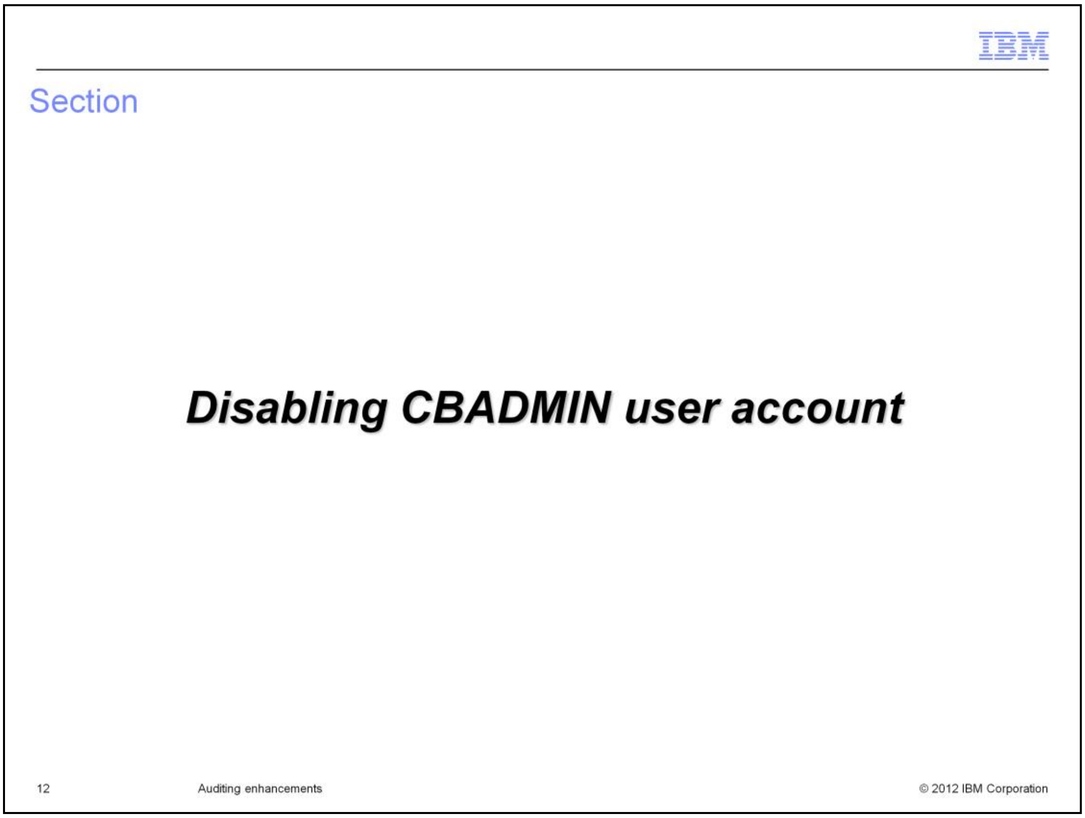
Auditing – read-only - user

- Logged on to “Audread” user
- Read-only allows auditor to:
  - Review event log utilization
  - Download (but not delete) auditing records

11 Auditing enhancements © 2012 IBM Corporation

When you log into IBM Workload Deployer as an auditor with read-only permissions, the menu dynamically matches your read-only permissions. While an “auditor with read-only permission” also has the permission “Deploy patterns in the cloud”, the primary function of the read-only auditor is to work with auditing records. The read-only auditor CANNOT manage auditing permissions for auditor users and groups. In fact, as you see in this example, **Users** and **User Groups** do not appear under the Systems pull-down menu.

The functionality to work with auditing records is available using the **Auditing** menu selection. Here an auditor can review the event log utilization and download log records (the same as a full permission auditor). However, a read-only auditor CANNOT delete auditing records.

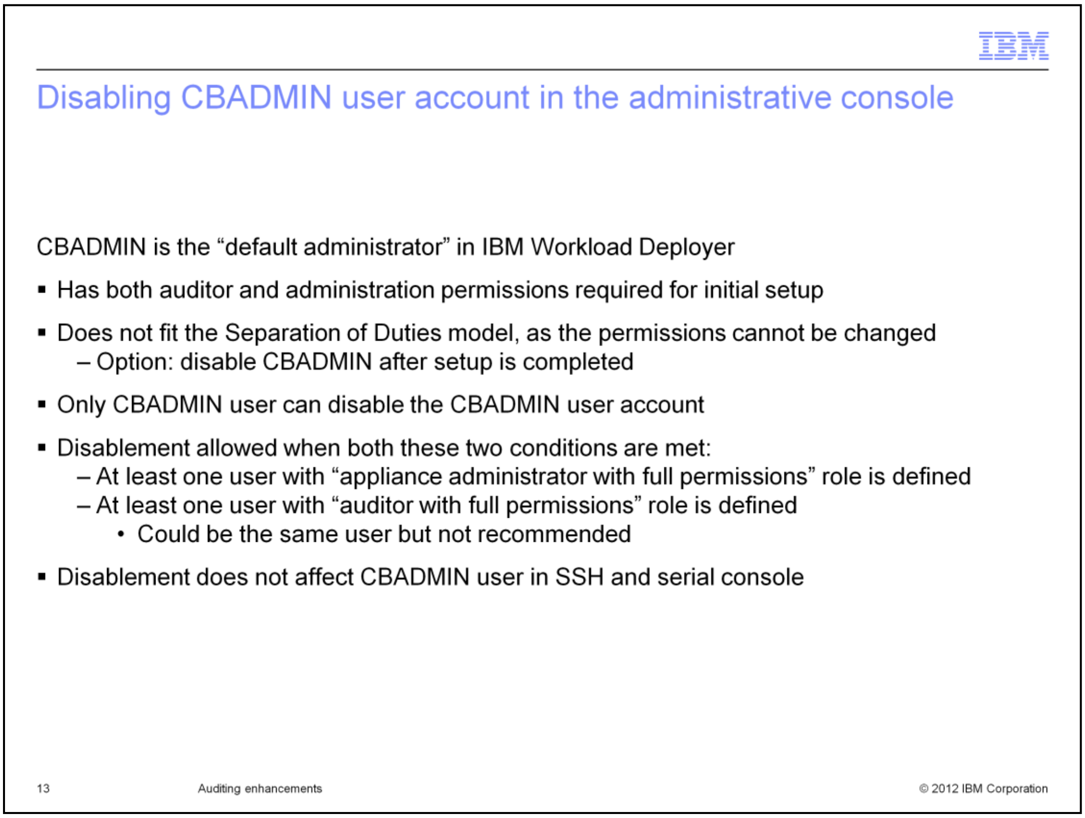


Section

Disabling CBADMIN user account

12 Auditing enhancements

This section discusses the disabling of the CBADMIN user account.



Disabling CBADMIN user account in the administrative console

CBADMIN is the “default administrator” in IBM Workload Deployer

- Has both auditor and administration permissions required for initial setup
- Does not fit the Separation of Duties model, as the permissions cannot be changed
  - Option: disable CBADMIN after setup is completed
- Only CBADMIN user can disable the CBADMIN user account
- Disablement allowed when both these two conditions are met:
  - At least one user with “appliance administrator with full permissions” role is defined
  - At least one user with “auditor with full permissions” role is defined
    - Could be the same user but not recommended
- Disablement does not affect CBADMIN user in SSH and serial console

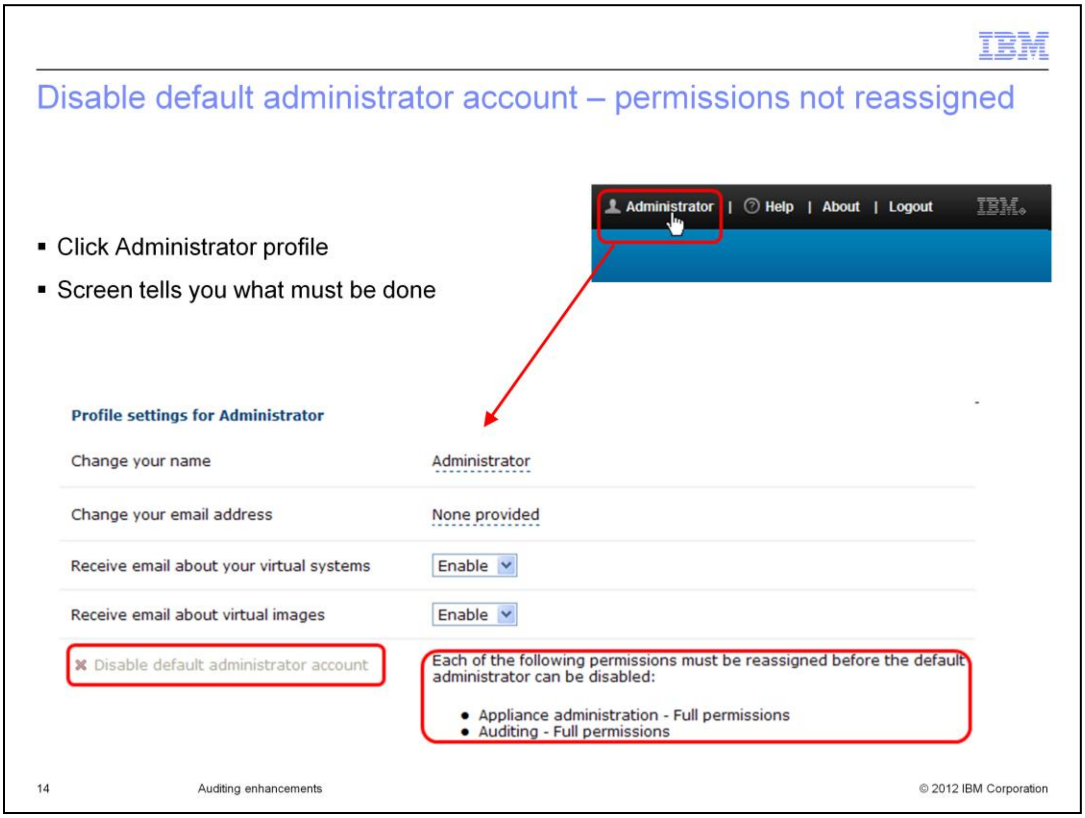
13 Auditing enhancements © 2012 IBM Corporation

The CBADMIN is the “default administrator” user account that is defined within the appliance and is used for the initial setup of the appliance. For this reason, it must have both the auditor and administration permissions. However, once the initial setup is completed, and after other necessary user accounts have been created, best practices in terms of the “separation of duties” model suggests that the CBADMIN user account be disabled.

Only CBADMIN user can disable the CBADMIN user account. Two conditions must be met for the disablement to complete successfully.

At least one user with “appliance administrator with full permissions” role is defined. At least one user with “auditor with full permissions” role is defined. And as previously stated, these two permissions can be held by the same user; however that is not recommended as it does not conform to the Separation of Duties best practice.

The disablement of CBADMIN does not affect SSH and serial console access to the appliance.



Disable default administrator account – permissions not reassigned

- Click Administrator profile
- Screen tells you what must be done

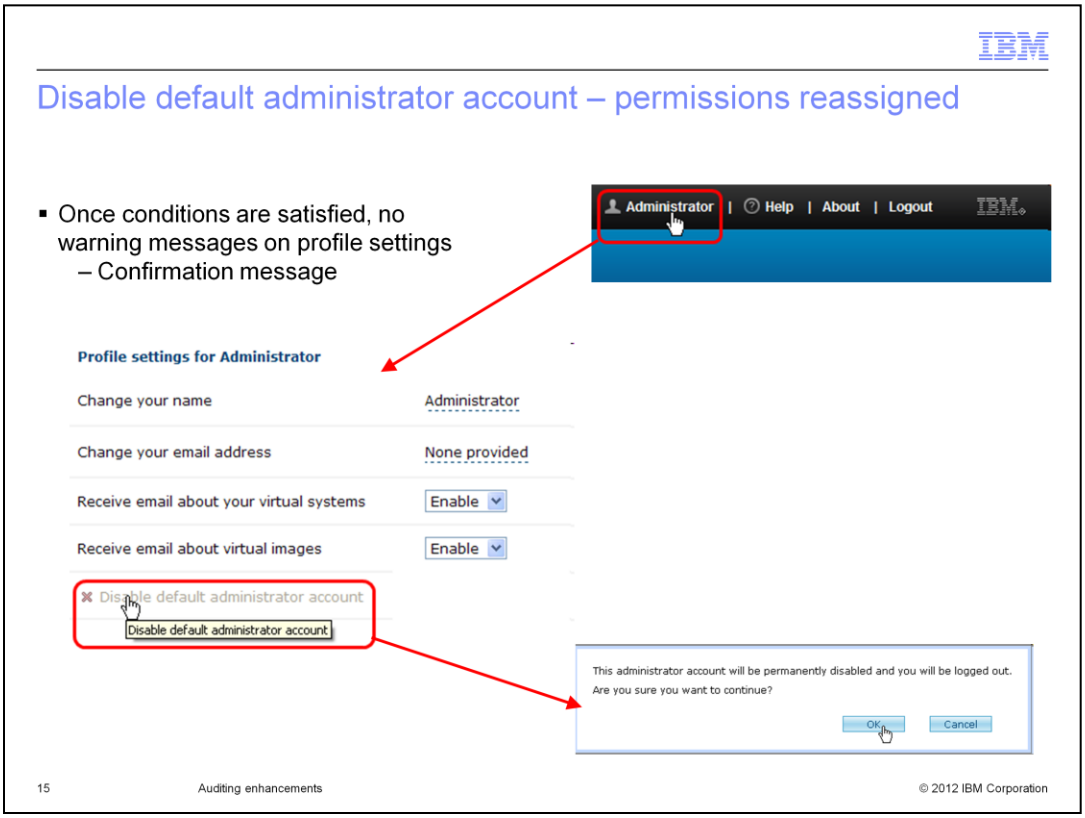
Profile settings for Administrator

Change your name	Administrator
Change your email address	None provided
Receive email about your virtual systems	Enable
Receive email about virtual images	Enable
✖ Disable default administrator account	Each of the following permissions must be reassigned before the default administrator can be disabled: ● Appliance administration - Full permissions ● Auditing - Full permissions

14 Auditing enhancements © 2012 IBM Corporation

To disable the CBADMIN account, you must be logged in with the CBADMIN user. From any screen, click Administrator on the top right of the screen. This navigates to the Profile Settings screen for the CBADMIN account.

The following two conditions must be met - at least one other user account must have “appliance administration with full permissions” and one other user account must have “auditing with full permissions”. If the conditions are not satisfied, then a message at the bottom right of the screen is displayed summarizing the required conditions, and the CBADMIN account disablement does not complete.



Disable default administrator account – permissions reassigned

- Once conditions are satisfied, no warning messages on profile settings
  - Confirmation message

Profile settings for Administrator

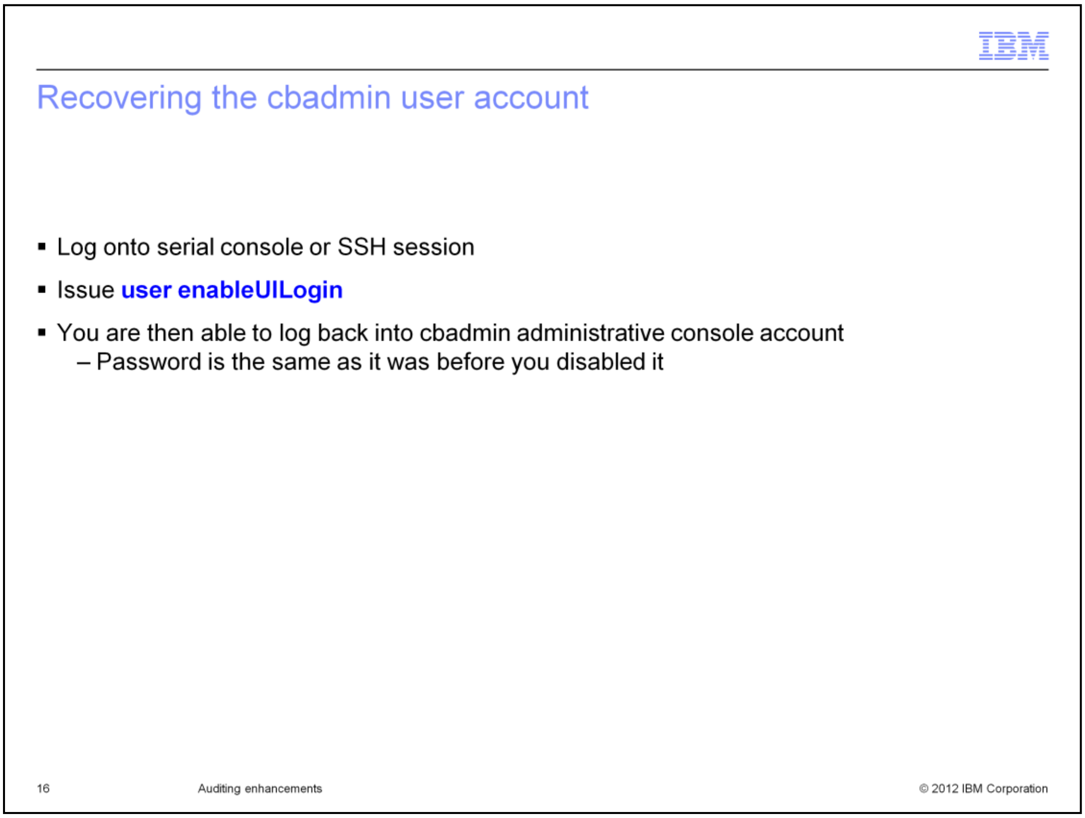
Change your name	Administrator
Change your email address	None provided
Receive email about your virtual systems	Enable
Receive email about virtual images	Enable

✖ Disable default administrator account
Disable default administrator account

This administrator account will be permanently disabled and you will be logged out.
Are you sure you want to continue?

15 Auditing enhancements © 2012 IBM Corporation

If the necessary permissions have been reassigned, the “Disable the default administrator account” function prompts you to confirm the disablement. This slide shows you an example of that prompt. Click **OK** to proceed with the disablement.

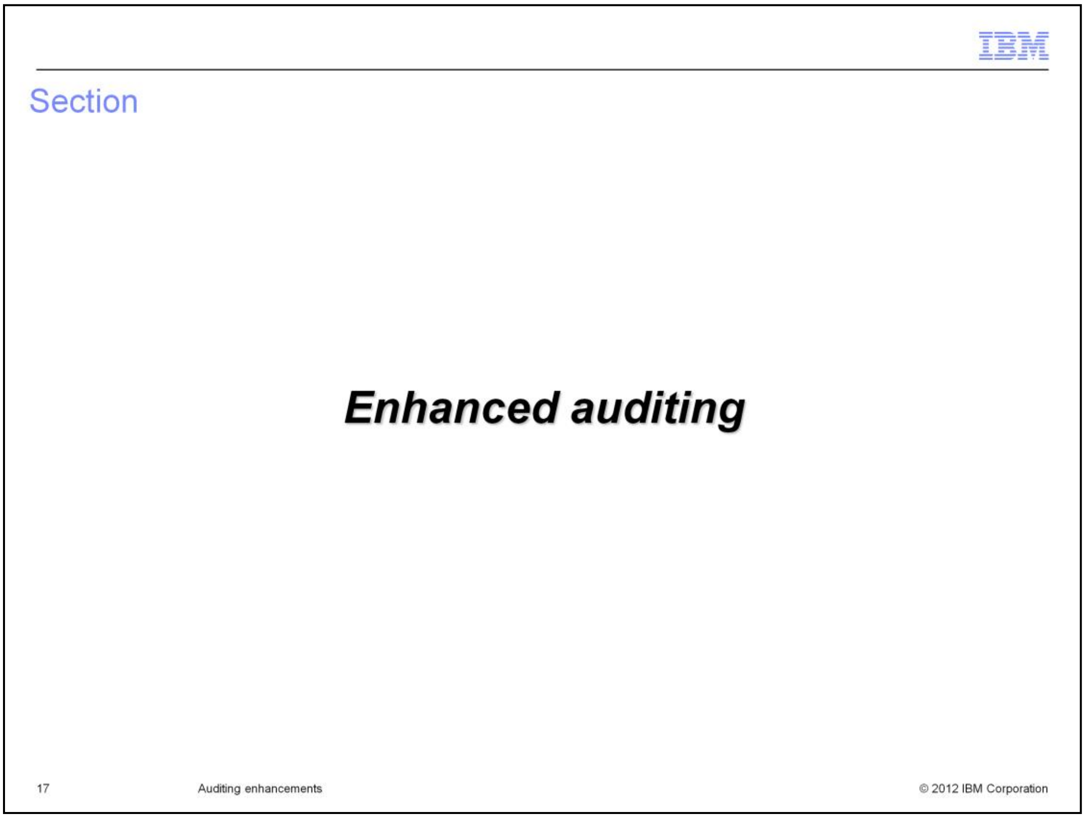


Recovering the cbadmin user account

- Log onto serial console or SSH session
- Issue **user enableUILogin**
- You are then able to log back into cbadmin administrative console account
  - Password is the same as it was before you disabled it

16 Auditing enhancements © 2012 IBM Corporation

If it becomes necessary to recover the CBADMIN user, then you can perform this enablement using an SSH login or a serial console login. Type the command **user enableUILogin**. The user account is re-enabled with the password it had when it was disabled.

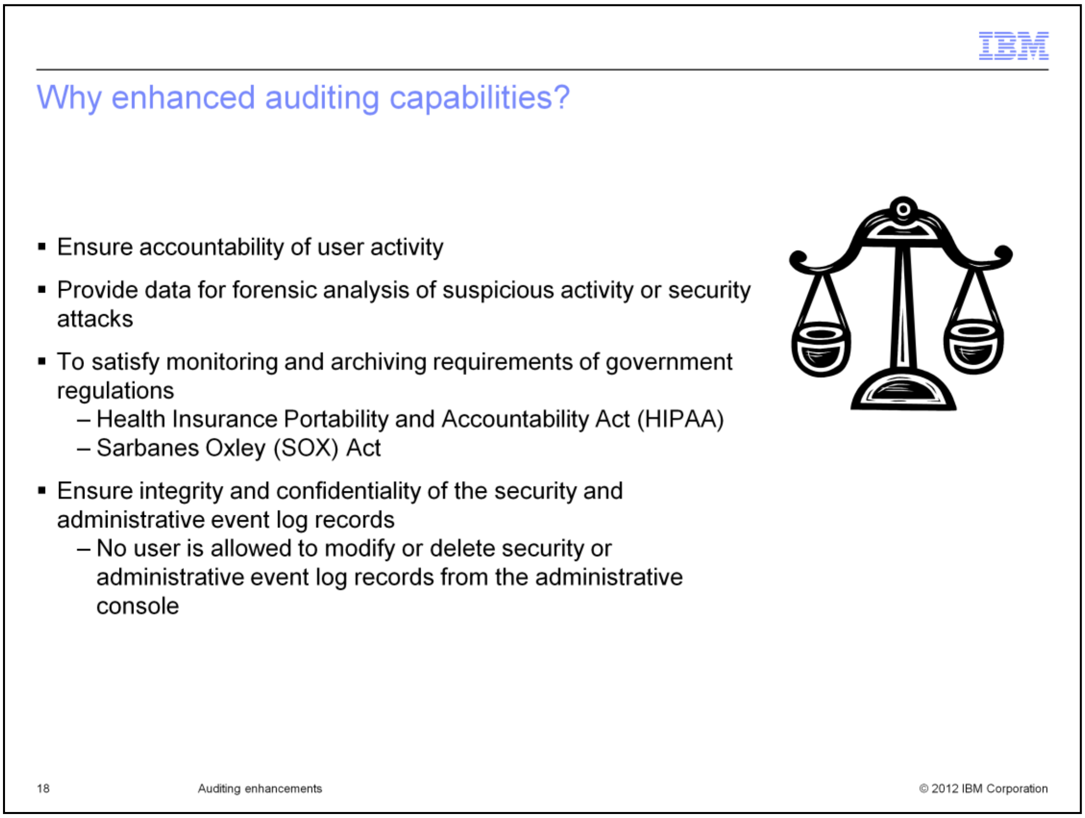


Section

Enhanced auditing

17 Auditing enhancements © 2012 IBM Corporation

This section discusses the enhancements to the auditing functionality.

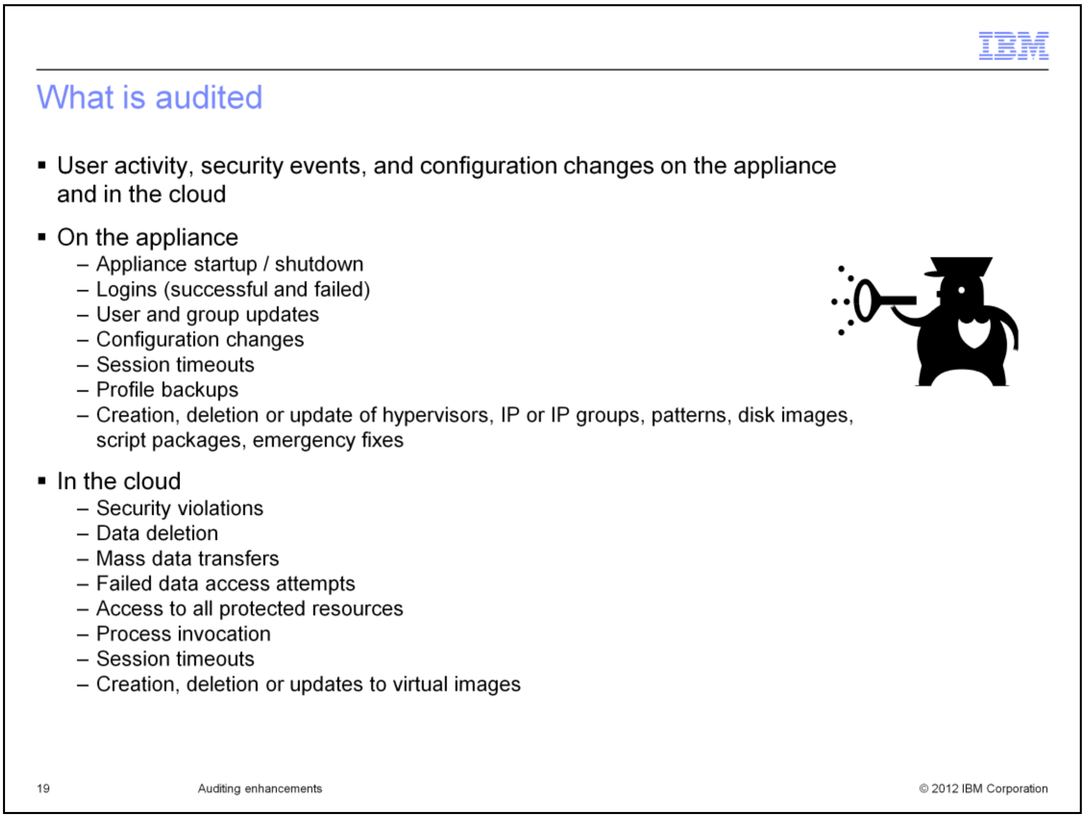


Why enhanced auditing capabilities?

- Ensure accountability of user activity
- Provide data for forensic analysis of suspicious activity or security attacks
- To satisfy monitoring and archiving requirements of government regulations
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Sarbanes Oxley (SOX) Act
- Ensure integrity and confidentiality of the security and administrative event log records
  - No user is allowed to modify or delete security or administrative event log records from the administrative console

18 Auditing enhancements © 2012 IBM Corporation

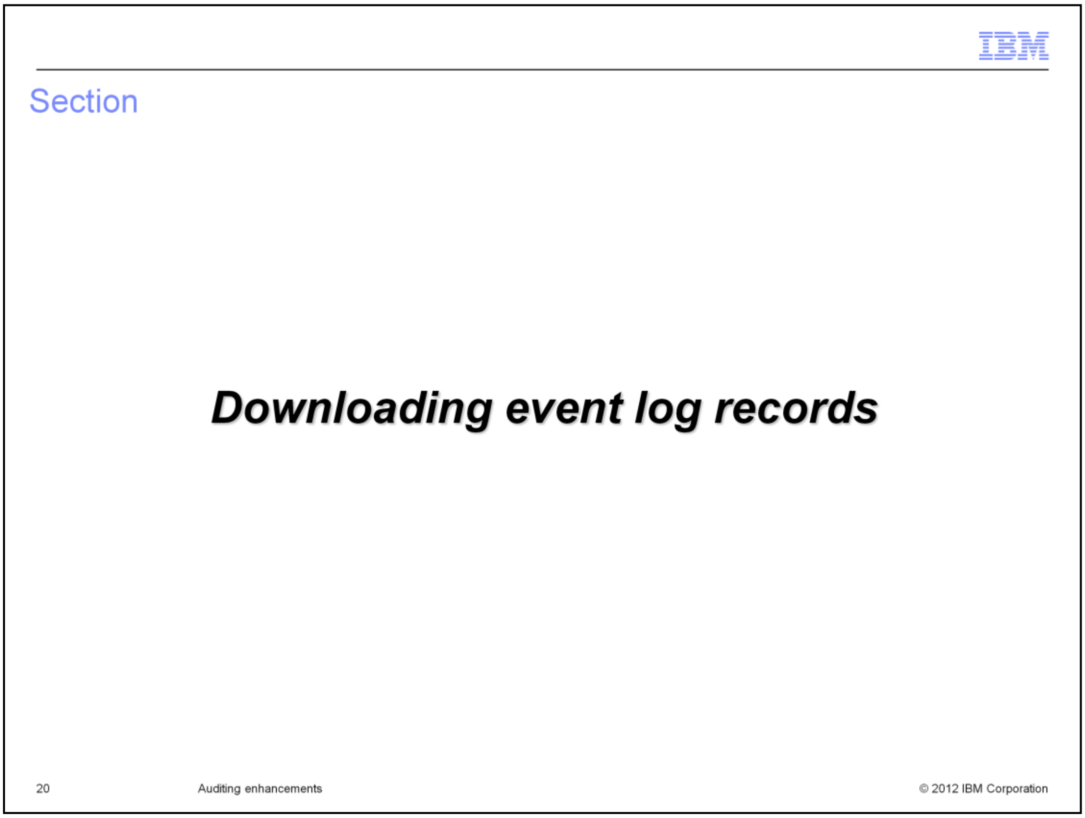
Auditing enhancements are implemented to ensure accountability of user activity. Provide data for forensic analysis of suspicious activity or security attacks. To satisfy requirements of governmental regulations. Ensure the integrity and confidentiality of the auditing and administrative event log records. And to ensure the integrity and confidentiality of the security and administrative event log records, no user is allowed to modify or delete the event log records from the administrative console.



What is audited

- User activity, security events, and configuration changes on the appliance and in the cloud
- On the appliance
  - Appliance startup / shutdown
  - Logins (successful and failed)
  - User and group updates
  - Configuration changes
  - Session timeouts
  - Profile backups
  - Creation, deletion or update of hypervisors, IP or IP groups, patterns, disk images, script packages, emergency fixes
- In the cloud
  - Security violations
  - Data deletion
  - Mass data transfers
  - Failed data access attempts
  - Access to all protected resources
  - Process invocation
  - Session timeouts
  - Creation, deletion or updates to virtual images

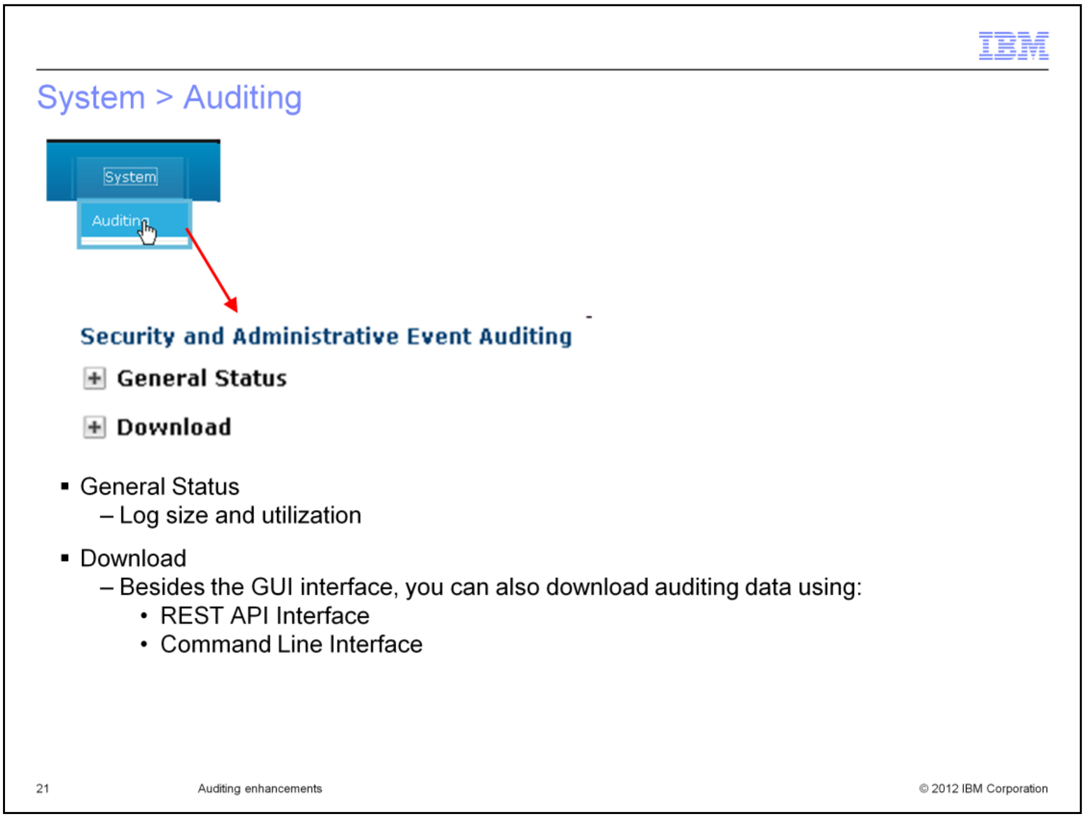
In general, the event log records include, User activity, such as successful or unsuccessful logins. Resource, definition or configuration changes. Security events and security changes. Process invocations and session timeouts. Profile backups. Data deletions. And access to all protected resources.



Section

Downloading event log records

This section discusses how to download the security and administrative event log records.



System > Auditing

Security and Administrative Event Auditing

⊞ General Status

⊞ Download

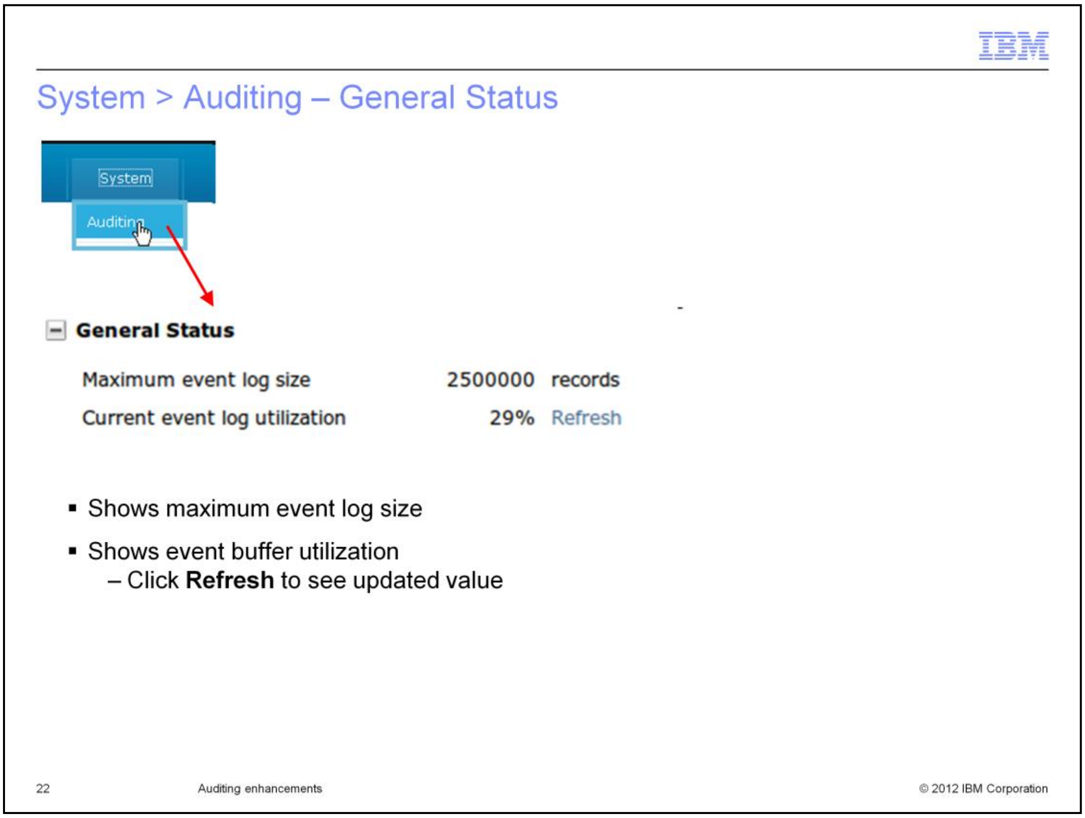
- General Status
  - Log size and utilization
- Download
  - Besides the GUI interface, you can also download auditing data using:
    - REST API Interface
    - Command Line Interface

21 Auditing enhancements © 2012 IBM Corporation

The three primary functions an auditor can do in regard to the auditing data collected on the appliance are, Review the event log usage, download event log records, and delete event log records.

This section focuses on reviewing log usage, under the **General Status** menu heading, and downloading the auditing data, under the **Download** menu heading. These two functions can be performed by an auditor with read-only permissions, and by an auditor with full permissions.

The downloading of auditing data can be done using the administrative console, using REST APIs, and using the Command Line Interface. You see information about all three techniques in this section.



System > Auditing – General Status

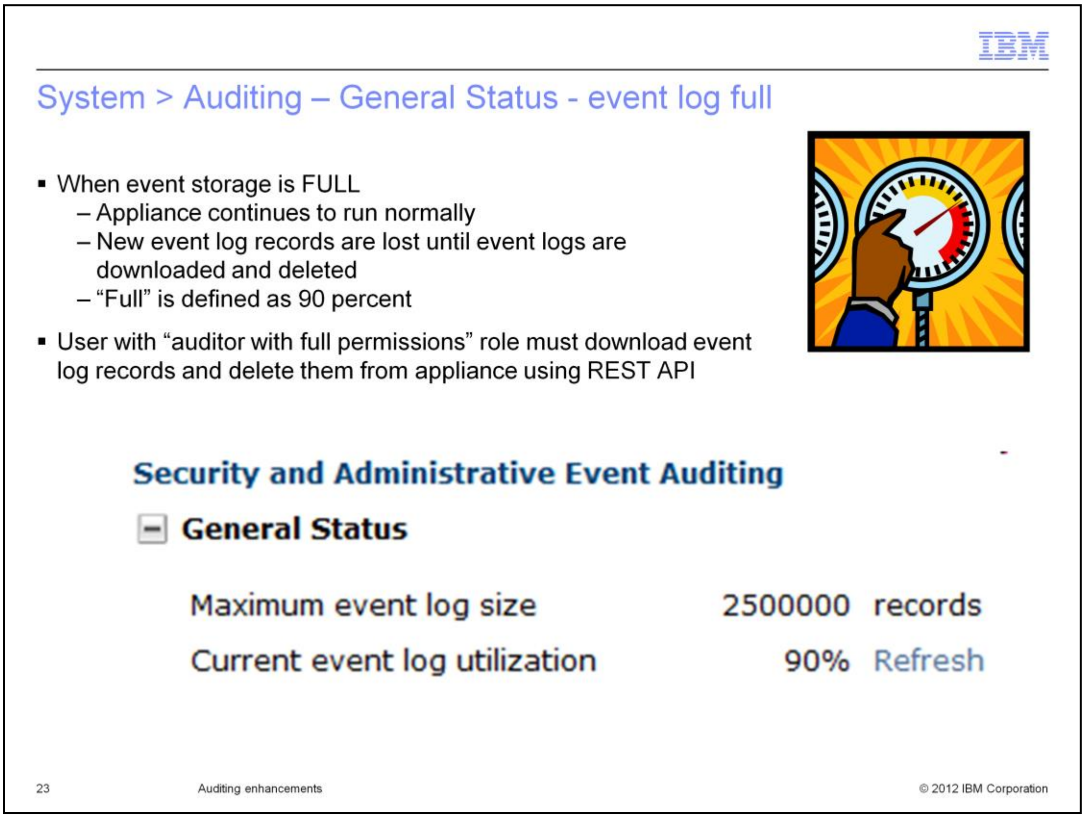
General Status

Maximum event log size	2500000	records
Current event log utilization	29%	Refresh

- Shows maximum event log size
- Shows event buffer utilization
  - – Click **Refresh** to see updated value

General Status provides the maximum event log size, which is fixed at 2,500,000 records. The current utilization of the log, along with a Refresh capability to see the updated value.

If you have displayed this screen for some time and think the log utilization value is stale, click the **Refresh** link to see a refreshed value.



IBM

System > Auditing – General Status - event log full

- When event storage is FULL
  - Appliance continues to run normally
  - New event log records are lost until event logs are downloaded and deleted
  - “Full” is defined as 90 percent
- User with “auditor with full permissions” role must download event log records and delete them from appliance using REST API

Security and Administrative Event Auditing

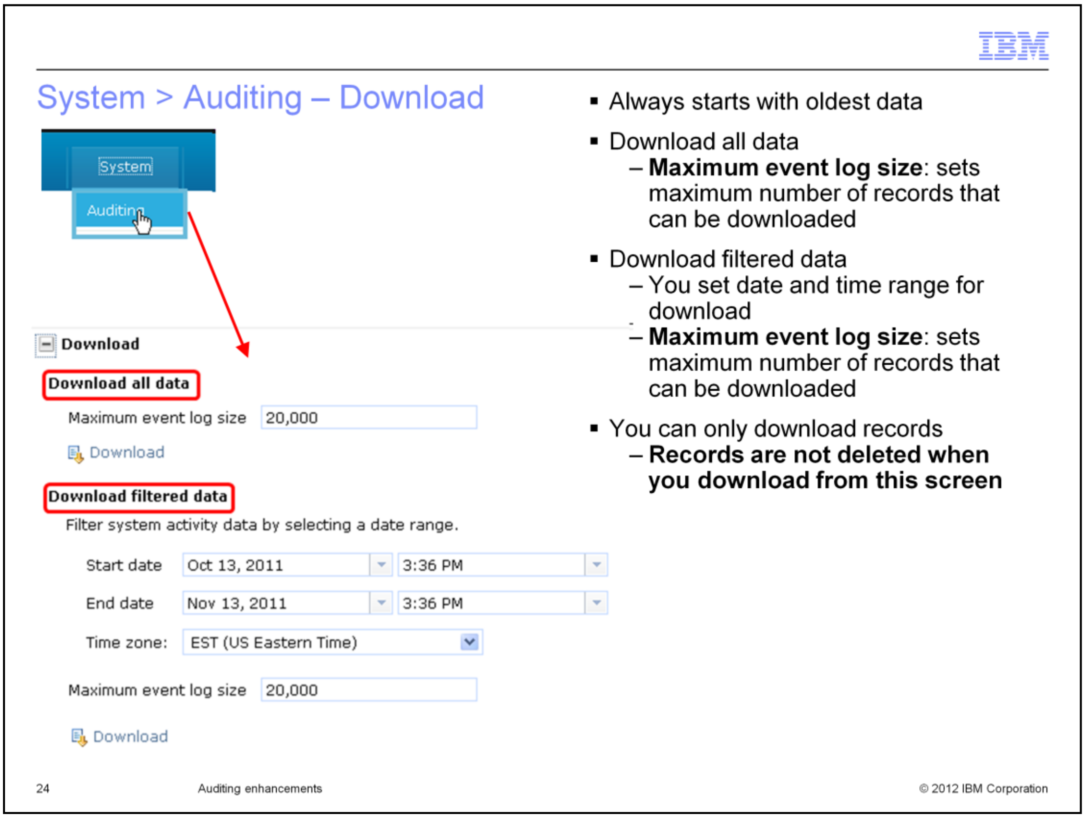
⊟ **General Status**

Maximum event log size	2500000	records
Current event log utilization	90%	Refresh

23 Auditing enhancements © 2012 IBM Corporation

If event log records are not deleted on a regular basis or not quickly enough, the event log might become full, where “full” is defined as 90 percent utilization. If this occurs, the appliance continues to run normally; however, all new auditing records are discarded.

It is necessary to download and delete enough auditing records to allow the automatic re-enablement of event logging. This is done with the provided sample scripts that use REST APIs.



System > Auditing – Download

Download

Download all data

Maximum event log size: 20,000

Download

Download filtered data

Filter system activity data by selecting a date range.

Start date: Oct 13, 2011 3:36 PM

End date: Nov 13, 2011 3:36 PM

Time zone: EST (US Eastern Time)

Maximum event log size: 20,000

Download

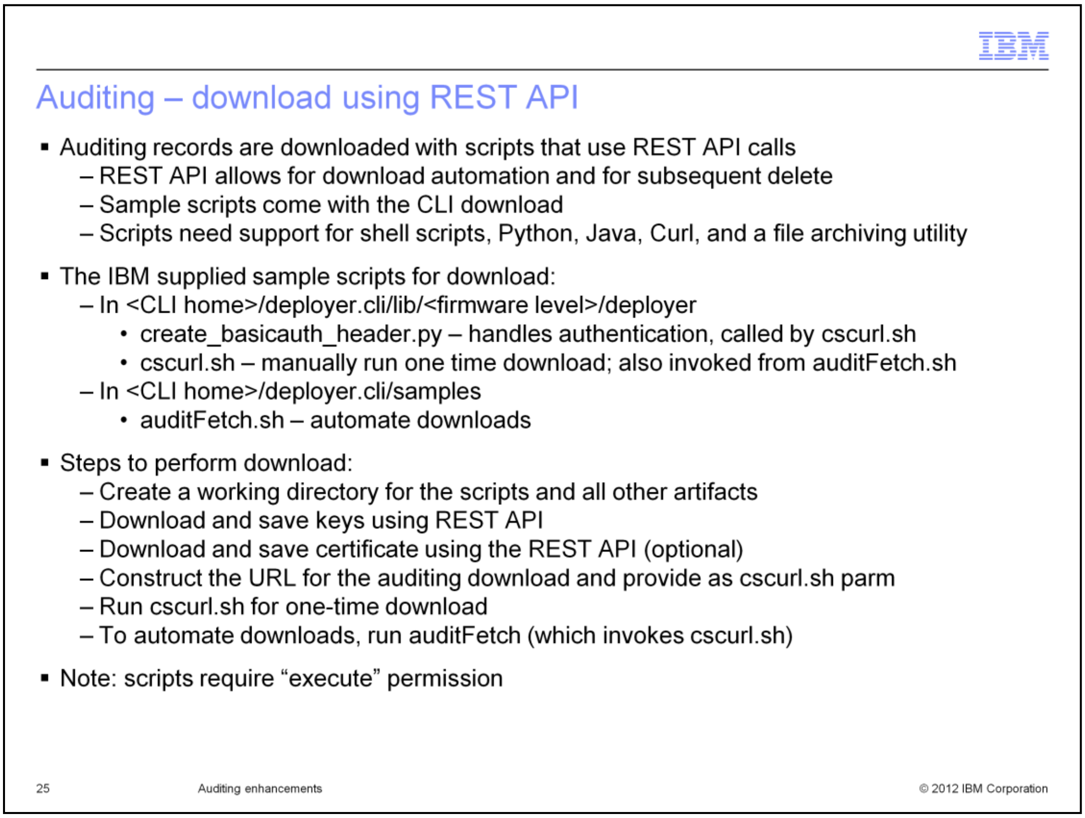
- Always starts with oldest data
- Download all data
  - **Maximum event log size**: sets maximum number of records that can be downloaded
- Download filtered data
  - You set date and time range for download
  - **Maximum event log size**: sets maximum number of records that can be downloaded
- You can only download records
  - **Records are not deleted when you download from this screen**

24 Auditing enhancements © 2012 IBM Corporation

The Download function provides two different ways to download event log records using the administrative console. Note that any processing of data in the event log always starts with the oldest data available.

The first option (Download all data) downloads the number of records requested, starting with the oldest records available. The default and maximum is 20,000 records. You should not immediately test the download function by attempting to download 20,000 records using the administrative console. Instead, try downloading a smaller number of records first, such as 100 records, so you can see the length of time that the download function requires.

The second option (Download filtered data) also downloads the number of records requested, but has the additional filter of a date and time stamp. The Time zone function is currently inactive and should be ignored. The **Download filtered data** downloads the oldest records within this date range. The default and maximum is 20,000 records over the past month starting from today. The time stamp within the downloaded records are in UTC. You should first try this download function with a small number of records, so you can predict the time required for downloading a larger number of records. Note that in both these types of downloads, no auditing records are deleted.



Auditing – download using REST API

- Auditing records are downloaded with scripts that use REST API calls
  - REST API allows for download automation and for subsequent delete
  - Sample scripts come with the CLI download
  - Scripts need support for shell scripts, Python, Java, Curl, and a file archiving utility
- The IBM supplied sample scripts for download:
  - In <CLI home>/deployer.cli/lib/<firmware level>/deployer
    - create_basicauth_header.py – handles authentication, called by cscurl.sh
    - cscurl.sh – manually run one time download; also invoked from auditFetch.sh
  - In <CLI home>/deployer.cli/samples
    - auditFetch.sh – automate downloads
- Steps to perform download:
  - Create a working directory for the scripts and all other artifacts
  - Download and save keys using REST API
  - Download and save certificate using the REST API (optional)
  - Construct the URL for the auditing download and provide as cscurl.sh parm
  - Run cscurl.sh for one-time download
  - To automate downloads, run auditFetch (which invokes cscurl.sh)
- Note: scripts require “execute” permission

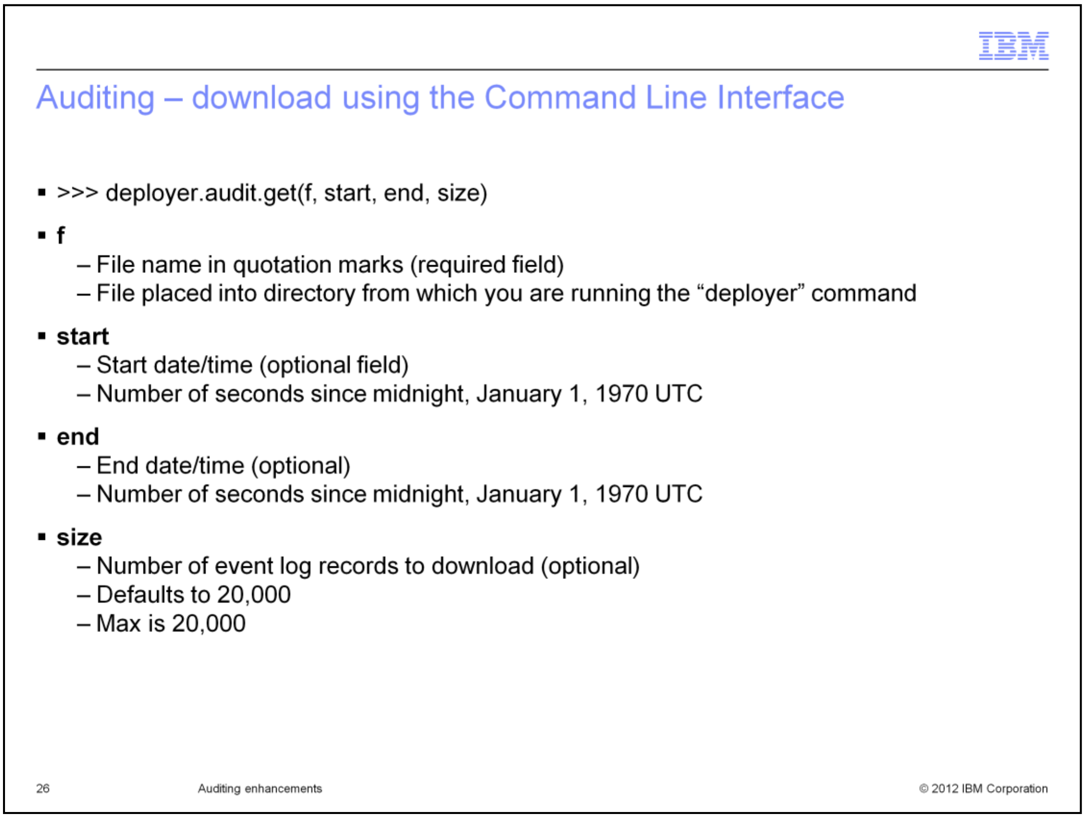
25 Auditing enhancements © 2012 IBM Corporation

Another way to download event log records are with a REST API. IBM has provided sample scripts utilizing the REST API for this type of download. These scripts come with the CLI download, and can be found in the directories in the slide. Two of the scripts involved are .sh scripts and require support for shell scripts, Python, Java, Curl, and a file archiving utility. The Linux environment is well suited for running the scripts. If you are running on Microsoft Windows, you must install software to provide a Linux-like environment to use these scripts for downloading event log records.

There are three scripts involved in this download process. Create_basicauth_header.py – Handles authentication using the user ID/password, the appliance keys, and optionally the appliance certificate; it is called by cscurl.sh. Cscurl.sh – This script is used for one-time downloads. It has numerous parameters passed to it, including the auditor user ID, password, appliance IP address, the key file, optionally the certificate file, the REST API URL, and an output file destination. Additionally it is invoked from the auditFetch.sh script. AuditFetch.sh – This script is used for automated downloads. From the parameters passed to it, it dynamically generates a REST API URL, and then invokes cscurl.sh with the correct parameters. The parameters passed to auditFetch.sh are: auditor user ID, password, key file, appliance IP address, the number of records to download, and an output file destination. Note that with this sample script, you cannot provide a time range for the download.

The steps to perform an event log download are provided above. Further details about each step are provided in the v3.1 Information Center, provided in the Reference slide at the end of the presentation.

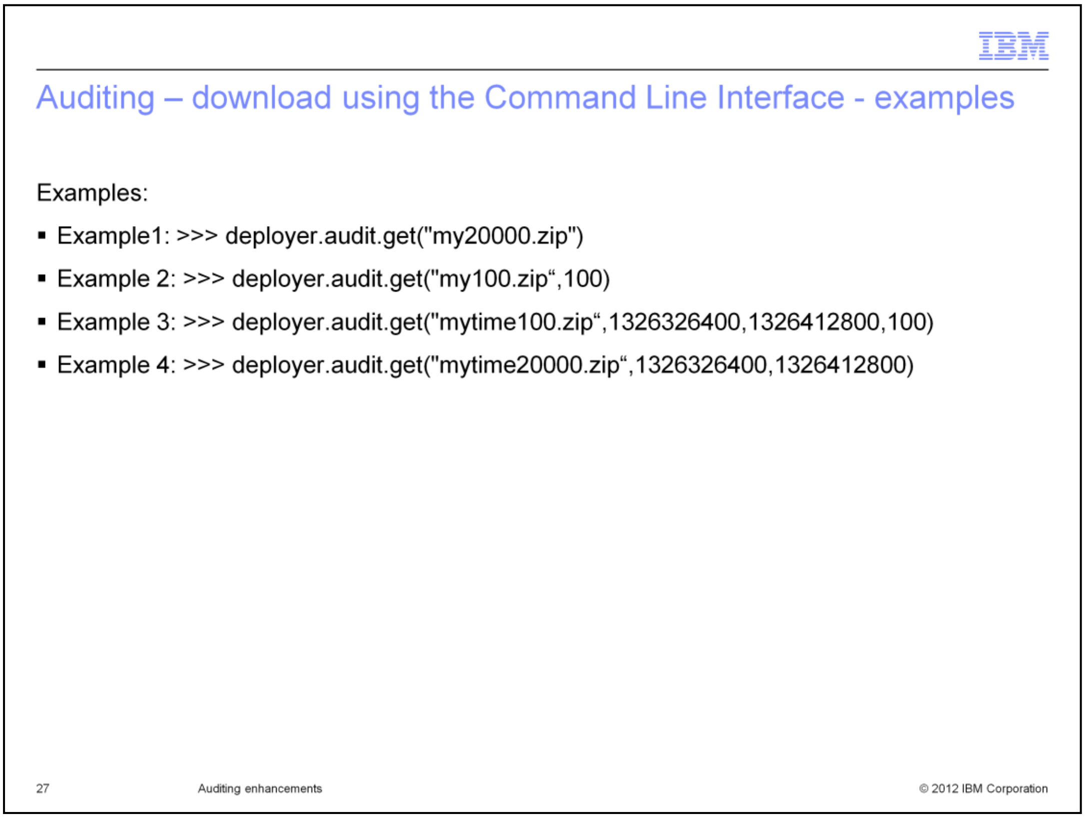
Note that if you are running on Linux, don’t forget to give “execute” permission to the scripts.



Auditing – download using the Command Line Interface

- >>> deployer.audit.get(f, start, end, size)
- **f**
  - File name in quotation marks (required field)
  - File placed into directory from which you are running the “deployer” command
- **start**
  - Start date/time (optional field)
  - Number of seconds since midnight, January 1, 1970 UTC
- **end**
  - End date/time (optional)
  - Number of seconds since midnight, January 1, 1970 UTC
- **size**
  - Number of event log records to download (optional)
  - Defaults to 20,000
  - Max is 20,000

The third way to download event log records is with the Command Line Interface. The basic format of the audit download command is provided in the first bullet of the foil. There are four parameters available for the command. The “f” parameter is the file name to be used as the download destination. It is a required parameter and is entered as text, in quotation marks. The location of this file is the same directory from which you are running the deployer command. If you want to filter by start and end times, then provide both the “start” and “end” parameters. Either both dates or no dates are to be provided; if only one date is provided, you will receive an error. The time is specified as the number of seconds since midnight, January 1, 1970 UTC. Note, in the near future, IBM plans to provide a downloadable tool to assist with calculating these times as seconds since midnight, January 1, 1970. The “size” parameter is the number of event log records to download. It is an optional field. The default and the maximum value is 20,000. If a larger number then 20,000 is given, the value is reduced to 20,000.

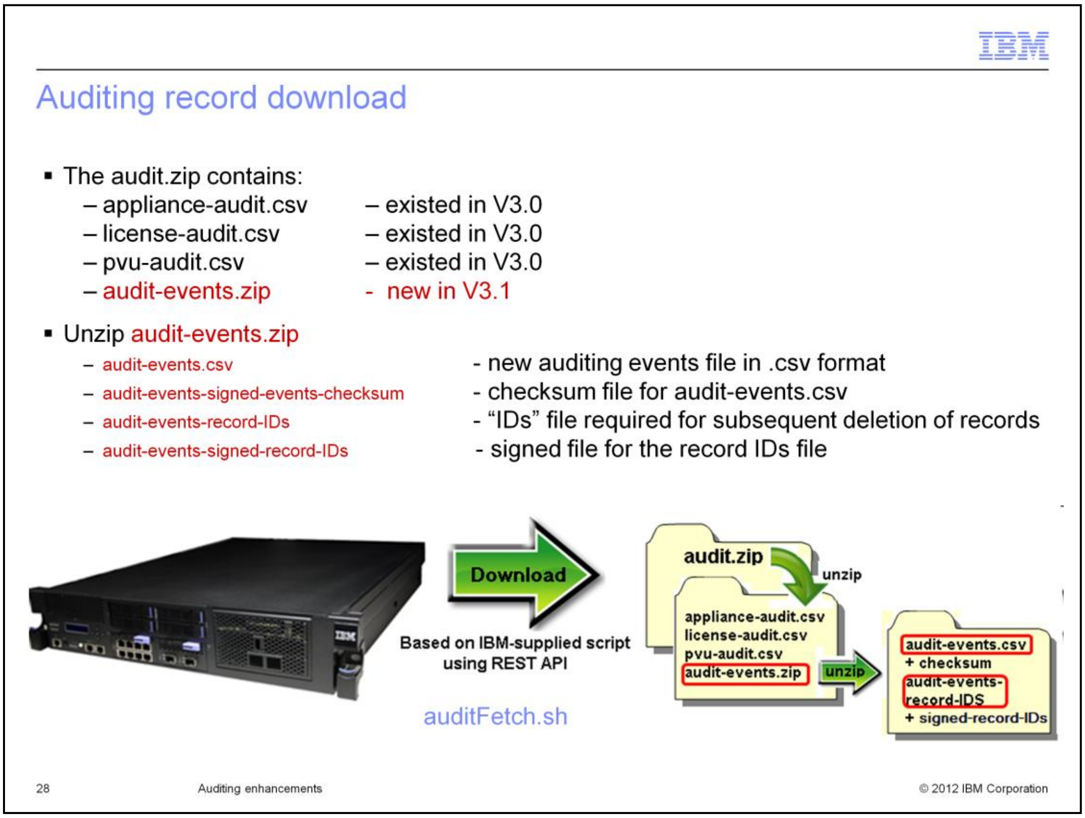


Auditing – download using the Command Line Interface - examples

Examples:

- Example1: >>> deployer.audit.get("my20000.zip")
- Example 2: >>> deployer.audit.get("my100.zip“,100)
- Example 3: >>> deployer.audit.get("mytime100.zip“,1326326400,1326412800,100)
- Example 4: >>> deployer.audit.get("mytime20000.zip“,1326326400,1326412800)

Here are some examples of Command Line Interface commands to download auditing event records. The first example provides the minimally required parameters to the command, specifically, the file name for the download. It will download up to the default 20,000 of the oldest records available in the event log. The second example is similar to the first example, except that the maximum number of records to be downloaded is 100. Up to 100 of the oldest records available are downloaded. The third example downloads the oldest 100 log records within the time frame provided. The start and end times in the example are from midnight January 12th, 2012 to midnight January 13th, 2012. The fourth example downloads up to 20,000 of the oldest records within the time frame provided. If less then 20,000 records are available within the time frame, then that lesser number is the number of records downloaded.



Auditing record download

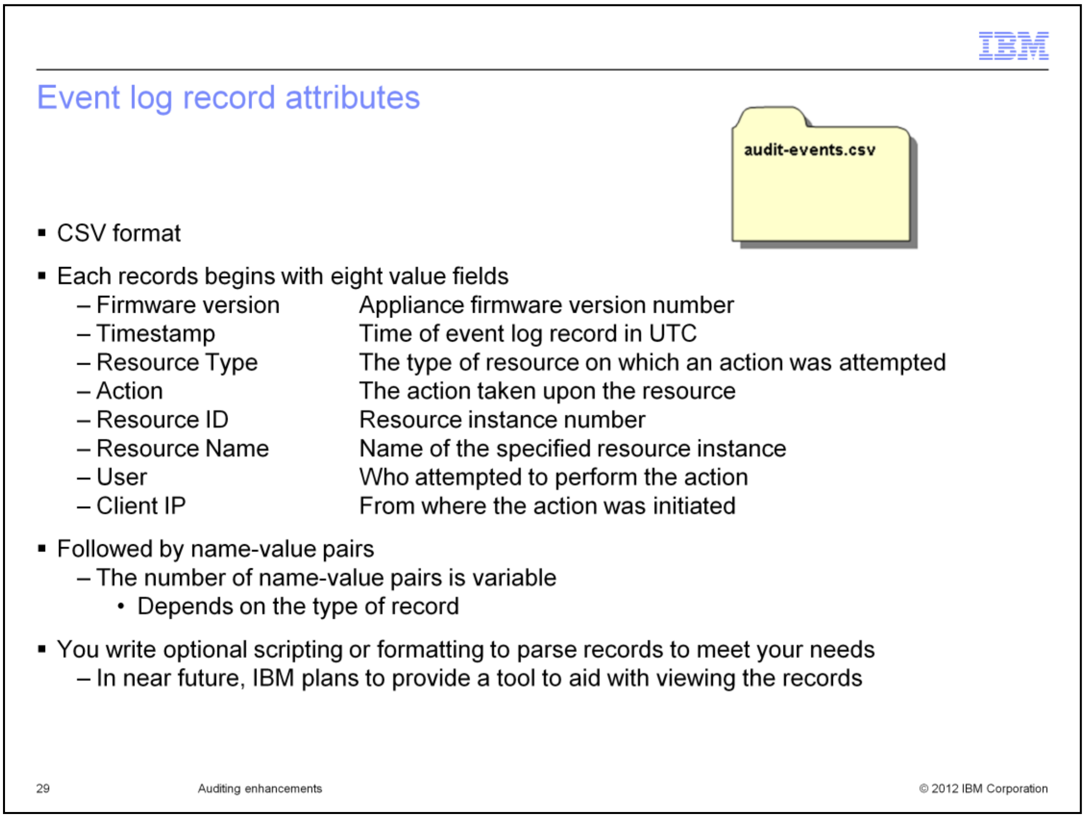
- The audit.zip contains:
  - – appliance-audit.csv – existed in V3.0
  - – license-audit.csv – existed in V3.0
  - – pvu-audit.csv – existed in V3.0
  - – audit-events.zip - new in V3.1
- Unzip audit-events.zip
  - – audit-events.csv - new auditing events file in .csv format
  - – audit-events-signed-events-checksum - checksum file for audit-events.csv
  - – audit-events-record-IDs - "IDs" file required for subsequent deletion of records
  - – audit-events-signed-record-IDs - signed file for the record IDs file

28 Auditing enhancements © 2012 IBM Corporation

Regardless of which of the three methods is used to download event log records, the result is the same. You retrieve a downloaded .zip file, named either the default audit.zip, or whatever name you provided in the REST API or the Command Line Interface. This .zip file has four files in it as follows.

Appliance-audit.csv: This file contains auditing records as provided in previous versions. **License-audit.csv:** The same auditing file as in v3.0 that contain all the licensing usage information. **Pvu-audit.csv**: The same auditing file as in v3.0 that contain all the pvu usage information. **Audit-events.zip**: The new v3.1 .zip file that contains the new security and administrative event log records.

The **audit-events.zip file** contains these four files, **Audit-events.csv**: Contains the new v3.1 auditing records in CSV format. These records are the ones discussed throughout this presentation. **Audit-events-signed-events-checksum**: Contains a signed checksum for the audit-events.csv file. Archive this file along with your audit-events.csv file. **Audit-event-record-IDs:** Contains the IDs for subsequent deletion of records. **Audit-events-signed-record-IDs:** Contains signature for the record IDs file for the subsequent deletion of records.



Event log record attributes

audit-events.csv

- CSV format
- Each records begins with eight value fields

– Firmware version	Appliance firmware version number
– Timestamp	Time of event log record in UTC
– Resource Type	The type of resource on which an action was attempted
– Action	The action taken upon the resource
– Resource ID	Resource instance number
– Resource Name	Name of the specified resource instance
– User	Who attempted to perform the action
– Client IP	From where the action was initiated

- Followed by name-value pairs
  - The number of name-value pairs is variable
    - Depends on the type of record
- You write optional scripting or formatting to parse records to meet your needs
  - In near future, IBM plans to provide a tool to aid with viewing the records

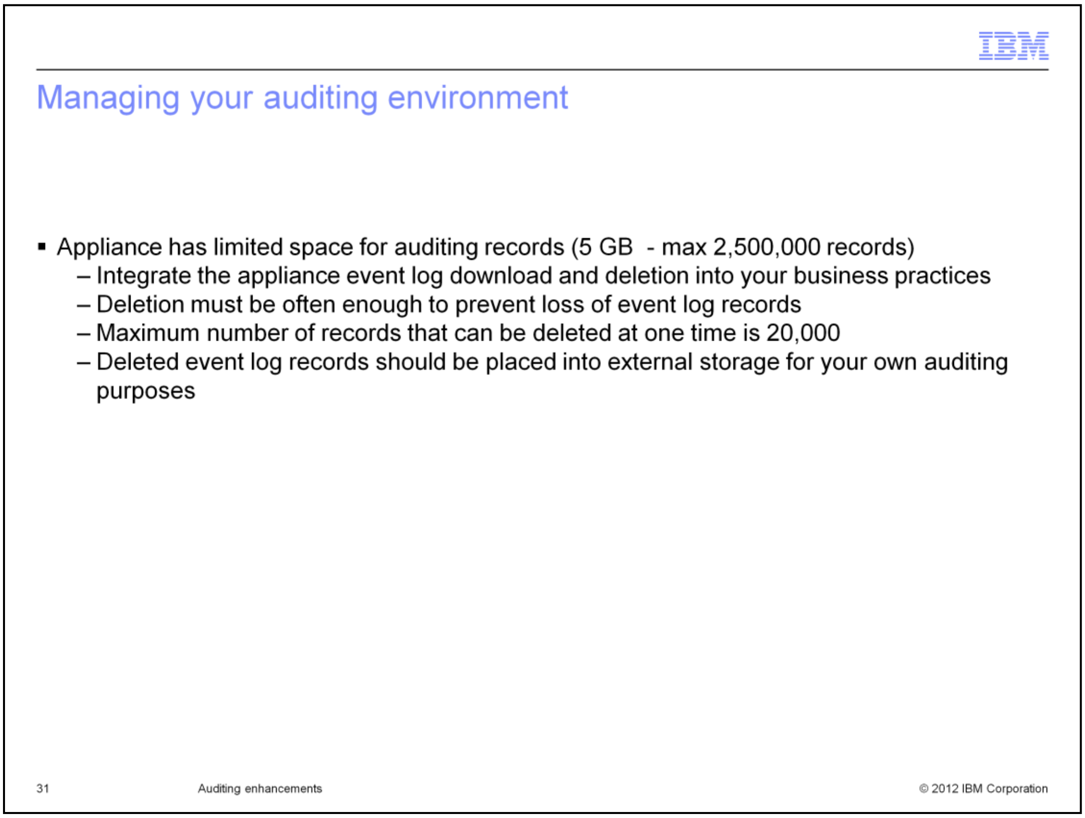
This slide discusses the **audit-events.csv** file that is new for IBM Workload Deployer V3.1. It is in CSV format. The first eight fields in every record are Firmware version, Timestamp (in UTC), Resource type, Action, Resource ID, Resource Name, User, and Client IP.

Following the standard header of eight fields, the types and number of fields varies based on the type of record. You must provide your own scripting to parse and format these records to meet your specific requirements. In the near future, IBM plans to provide a tool to help you view the records.

Section

Deleting event log records

This section will discuss how you delete event log records.



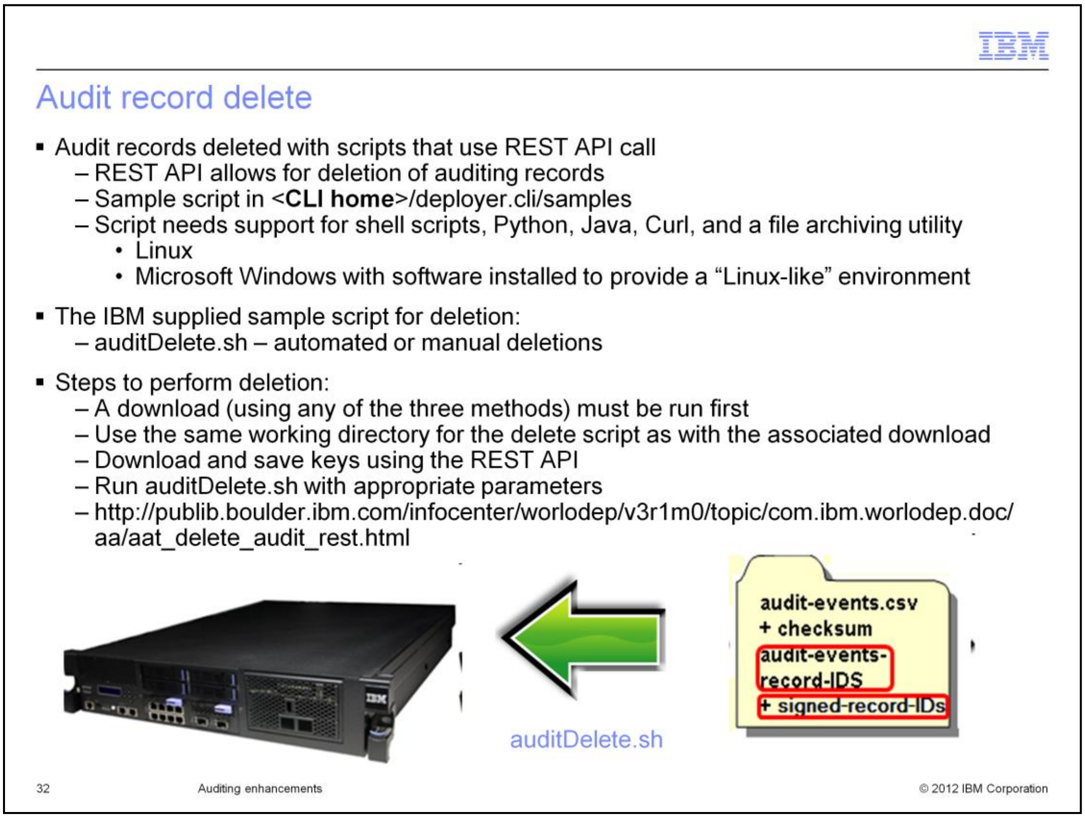
Managing your auditing environment

- Appliance has limited space for auditing records (5 GB - max 2,500,000 records)
  - Integrate the appliance event log download and deletion into your business practices
  - Deletion must be often enough to prevent loss of event log records
  - Maximum number of records that can be deleted at one time is 20,000
  - Deleted event log records should be placed into external storage for your own auditing purposes

31 Auditing enhancements

The IBM Workload Deployer appliance has a fixed size of five gigabytes available for the auditing records. This allows the storage of an average of 2,500,000 auditing records. Once this space has reached 90 percent utilization, no new auditing records are stored on the appliance. When that occurs, you must download and delete auditing records in order for auditing to resume. Therefore it is critical that a download and deletion process is integrated into your business practices.

Deletion of the auditing records must be often enough to ensure you never lose any auditing records. The maximum number of records that can be deleted at one time is 20,000, and only one delete can be running at any one time. Deleted auditing records and the associated checksum file should be archived into external storage for your own auditing requirements.



Audit record delete

- Audit records deleted with scripts that use REST API call
  - REST API allows for deletion of auditing records
  - Sample script in <**CLI home**>/deployer.cli/samples
  - Script needs support for shell scripts, Python, Java, Curl, and a file archiving utility
    - Linux
    - Microsoft Windows with software installed to provide a “Linux-like” environment
- The IBM supplied sample script for deletion:
  - auditDelete.sh – automated or manual deletions
- Steps to perform deletion:
  - A download (using any of the three methods) must be run first
  - Use the same working directory for the delete script as with the associated download
  - Download and save keys using the REST API
  - Run auditDelete.sh with appropriate parameters
  - http://publib.boulder.ibm.com/infocenter/worlodep/v3r1m0/topic/com.ibm.worlodep.doc/aa/aat_delete_audit_rest.html

audit-events.csv
+ checksum
audit-events-record-IDS
+ signed-record-IDs

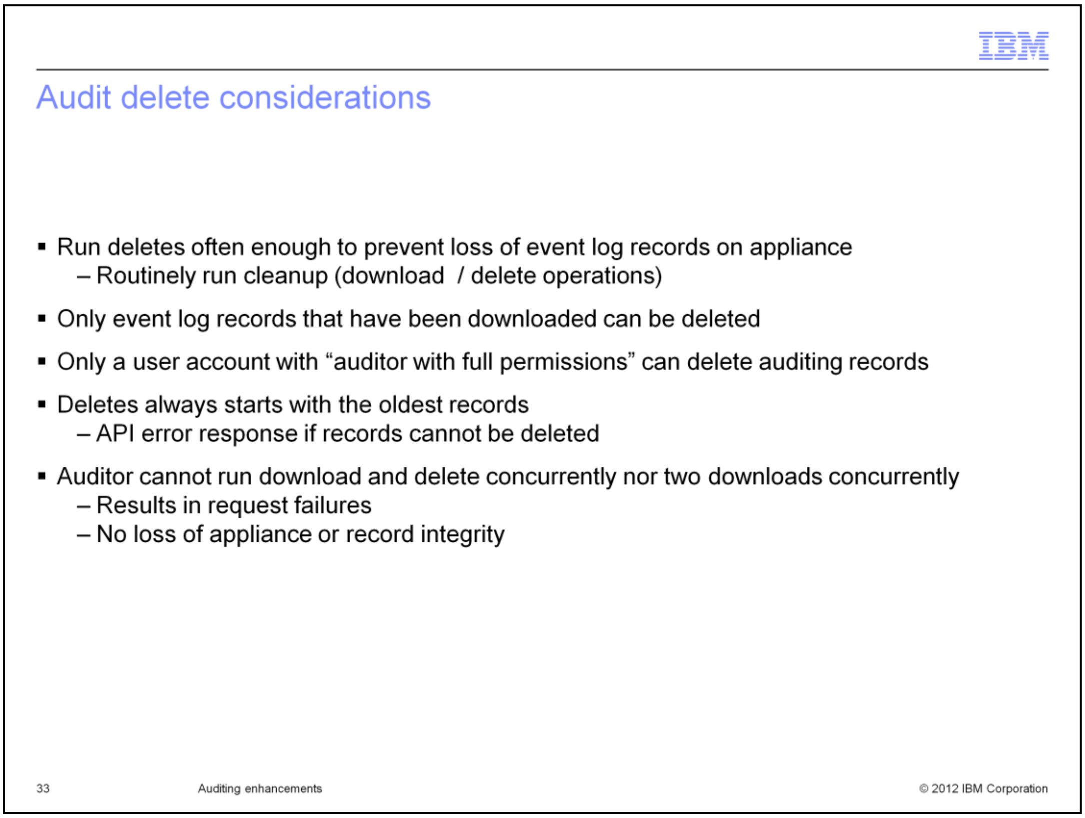
auditDelete.sh

Regardless of which of the three methods was used to download event log records, the deletion of the records requires the use of the REST API. In addition, the delete must be run by a user account that has “auditing with full permissions”. IBM provides a sample auditDelete.sh script which uses the REST API for this deletion. The script is provided within the Command Line Tool download in the directory in the slide.

The auditDelete.sh script requires support for shell scripts, Python, Java, and Curl. In addition, you likely want to store the files long-term in a file archiving facility. If you are running on Linux, you should be able to run the scripts without additional software. Remember to give the necessary “execute” and “read” permissions to the appropriate files before you invoke the scripts. If you are running on Microsoft Windows, you must install additional software to provide a “Linux-like environment” in order to use the auditDelete.sh script.

The auditDelete.sh script minimally requires these parameters: auditor user ID and password, the keys file, and the appliance IP address. Requires the **audit-events-record-IDs** file and the **audit-events-signed-records-IDs** file from the download, either passed as parameters to the script or located in the same directory as the script invocation.

Further details about the delete process are provided in the v3.1 Information Center.

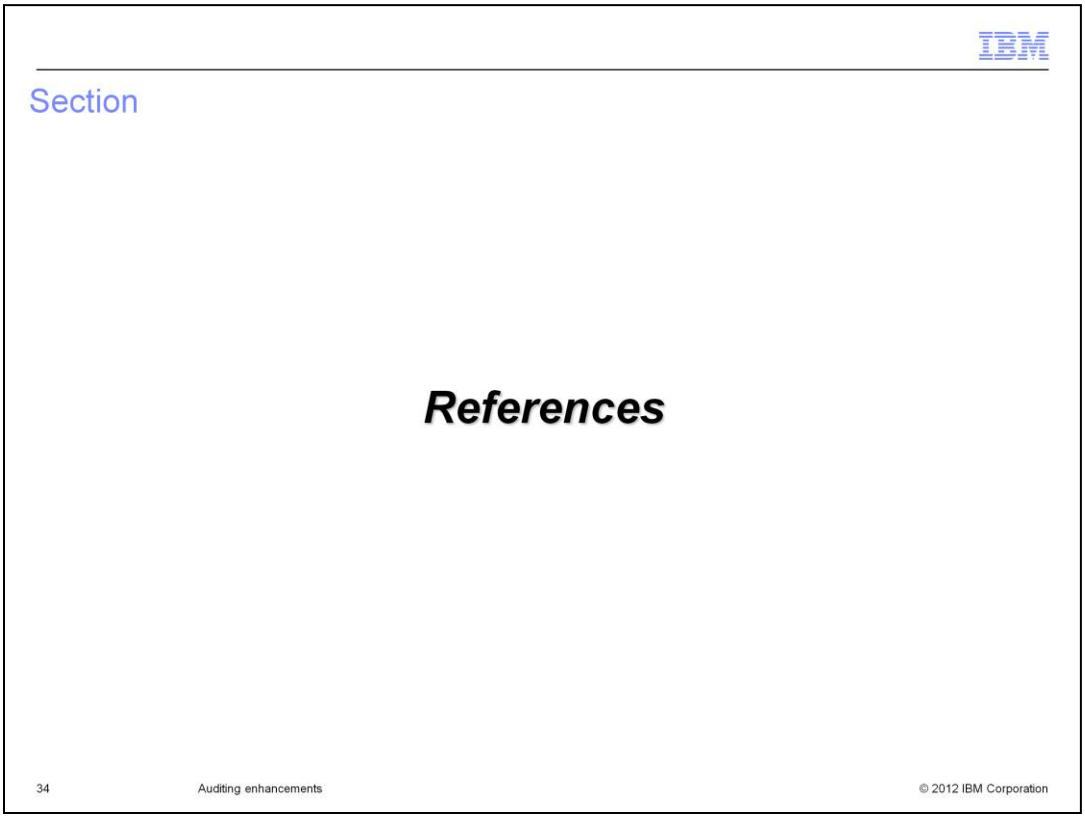


Audit delete considerations

- Run deletes often enough to prevent loss of event log records on appliance
  - Routinely run cleanup (download / delete operations)
- Only event log records that have been downloaded can be deleted
- Only a user account with “auditor with full permissions” can delete auditing records
- Deletes always starts with the oldest records
  - API error response if records cannot be deleted
- Auditor cannot run download and delete concurrently nor two downloads concurrently
  - Results in request failures
  - No loss of appliance or record integrity

Here is a summary of the auditing delete considerations.

Run auditing record retrieval and delete operations routinely to avoid the loss of event log records on the appliance. Only event log records that have been downloaded can be deleted. Only a user account with “auditor with full permissions” can delete auditing records. The delete function always starts with the oldest records. You receive an API error response if the records cannot be deleted. Auditors cannot run concurrent downloads or deletes (or any combination thereof) of auditing records. This results in a download or delete failure, although there is no loss of appliance or record integrity.

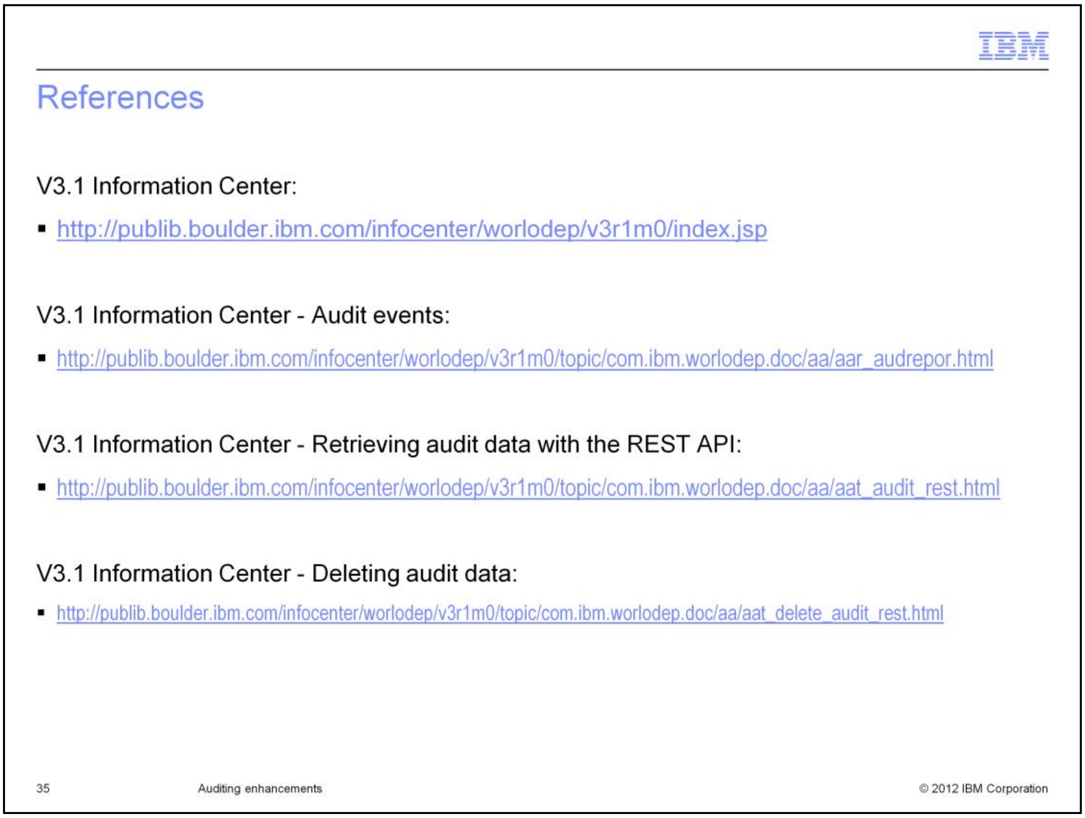


Section

References

34 Auditing enhancements © 2012 IBM Corporation

This section displays helpful references.



References

V3.1 Information Center:

- http://publib.boulder.ibm.com/infocenter/worlodep/v3r1m0/index.jsp

V3.1 Information Center - Audit events:

- http://publib.boulder.ibm.com/infocenter/worlodep/v3r1m0/topic/com.ibm.worlodep.doc/aa/aar_audrepor.html

V3.1 Information Center - Retrieving audit data with the REST API:

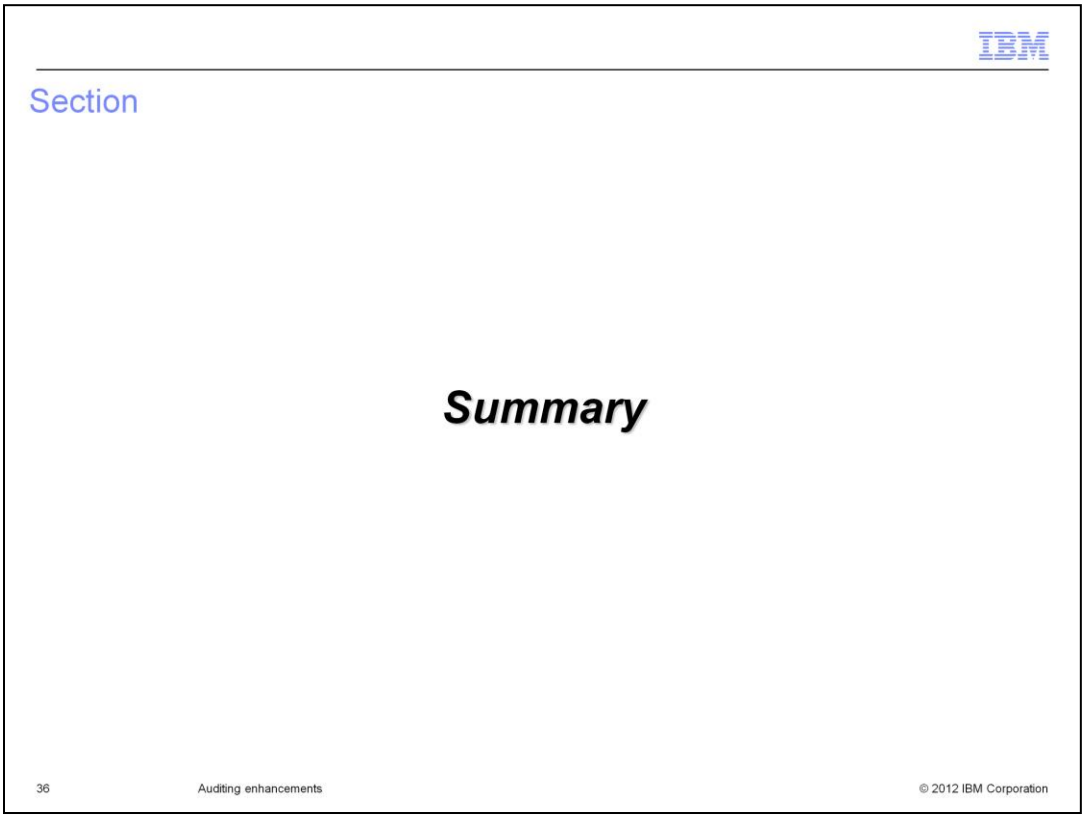
- http://publib.boulder.ibm.com/infocenter/worlodep/v3r1m0/topic/com.ibm.worlodep.doc/aa/aat_audit_rest.html

V3.1 Information Center - Deleting audit data:

- http://publib.boulder.ibm.com/infocenter/worlodep/v3r1m0/topic/com.ibm.worlodep.doc/aa/aat_delete_audit_rest.html

35 Auditing enhancements © 2012 IBM Corporation

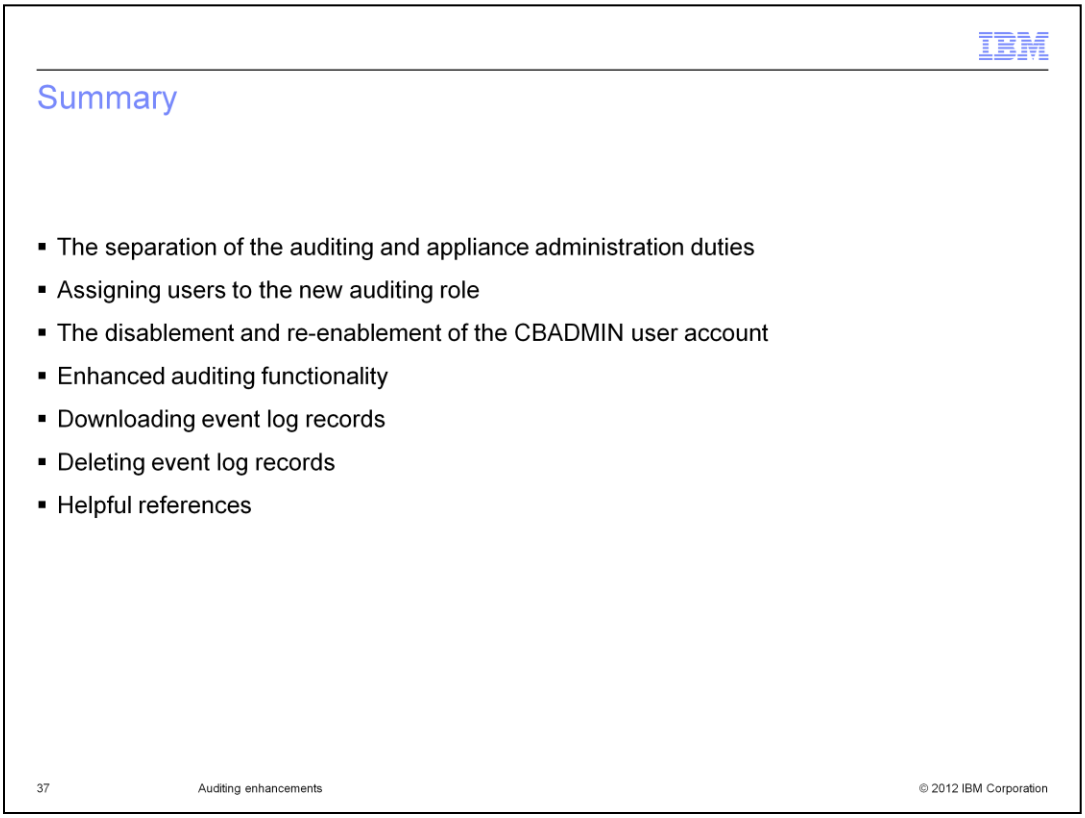
Click stop on this slide if you want to copy this information. Here are some references to resources that should help you understand and use the new auditing facility more effectively.



Section

Summary

This section provides a summary of the presentation.

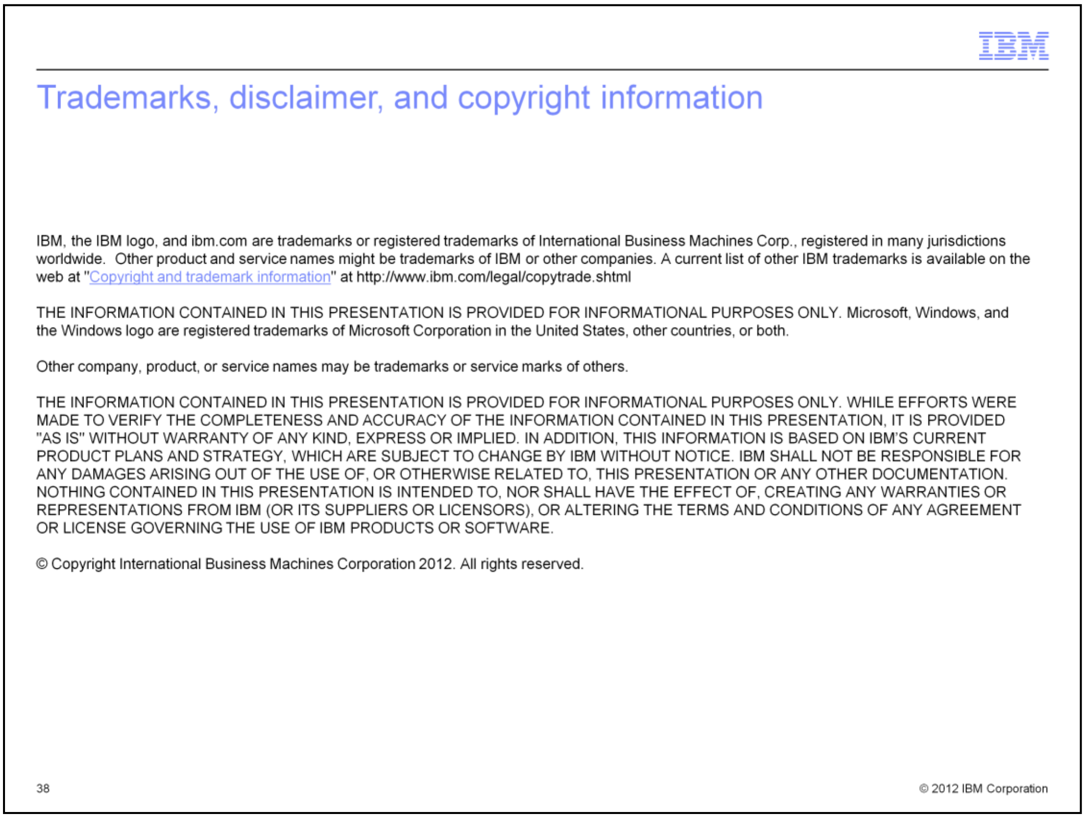


Summary

- The separation of the auditing and appliance administration duties
- Assigning users to the new auditing role
- The disablement and re-enablement of the CBADMIN user account
- Enhanced auditing functionality
- Downloading event log records
- Deleting event log records
- Helpful references

37 Auditing enhancements © 2012 IBM Corporation

You now should understand the importance of separating the auditing and appliance administration duties. You saw how the auditor user accounts are created and how they acquire the necessary permissions. The CBADMIN user account can now be optionally disabled, which removes a power user account from the appliance, to allow a better separation of duties for appliance administrators and auditors user accounts. A summary of the enhanced auditing functionality showed you important new auditing features available in IBM Workload Deployer V3.1. You saw how to download and delete event log records. Finally, you saw references to resources that should help you use the auditing facility effectively.



Trademarks, disclaimer, and copyright information

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. Microsoft, Windows, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.