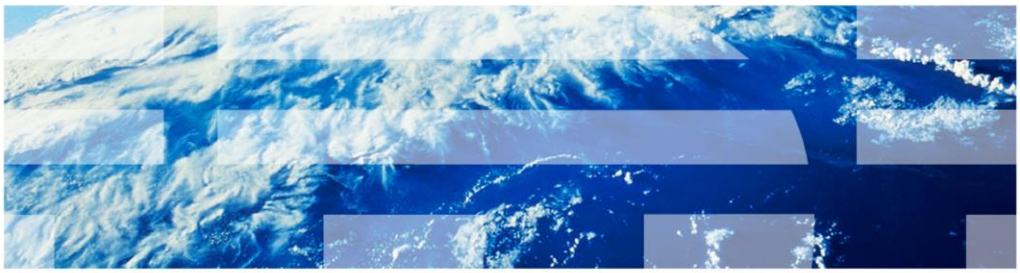
IBM PureApplication System

Auditing



© 2012 IBM Corporation

This presentation discusses the auditing function in IBM PureApplication™ System.

Agenda - Auditing

- Separation of duties
- Assigning users to the auditing role
- Auditing functions
- Management of audit records
- Summary

© 2012 IBM Corporation

This presentation discusses:

The separation of the auditing and PureApplication System administration duties, assigning users to the auditing role. auditing functions, management of audit records, and a summary of this presentation.

Section

Separation of duties

© 2012 IBM Corporation

This section discusses the separation of duties in respect to the auditing role.

The auditing role

- Auditor role with two levels of permissions
  - "Manage auditing (Full permission)"
  - "View all auditing reports (Read-only)"
- Allows separation of auditing from PureApplication System administrators
  - Auditor accesses auditing features only
    - Administrative roles should not audit
    - Auditor roles should not administer PureApplication System
- First admin user account assigns permissions for first auditor, granting:
  - Read plus "configure" capabilities for auditing
    - "Manage Auditing (Full permission)"
  - Permission to create or manage other auditors
    - "Delegation" permission is additionally required

4 Auditing © 2012 IBM Corporation

PureApplication System 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 PureApplication System.

PureApplication System provides an auditor role for this purpose. Within the auditor role, there are two levels of permissions – "Manage auditing (Full permission)" and "View all auditing reports (Read-only)".

Further, this separation of duties affects how permissions are granted to other users. The first admin user account must set the permissions for the first auditor user with "Manage auditing (Full permission)" and with "Delegation" permission. After that, the auditor with "Full permission" and "Delegation" permission can assign or revoke auditing permission for other users.

Section

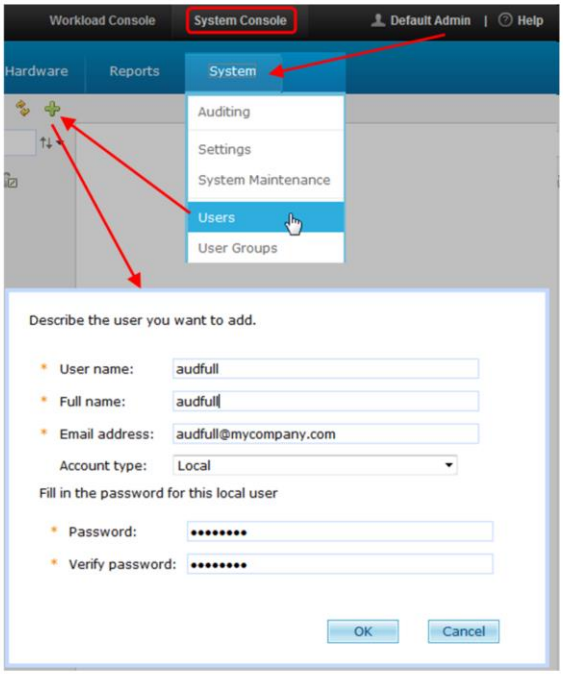
Assigning users to the new auditing role

© 2012 IBM Corporation

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

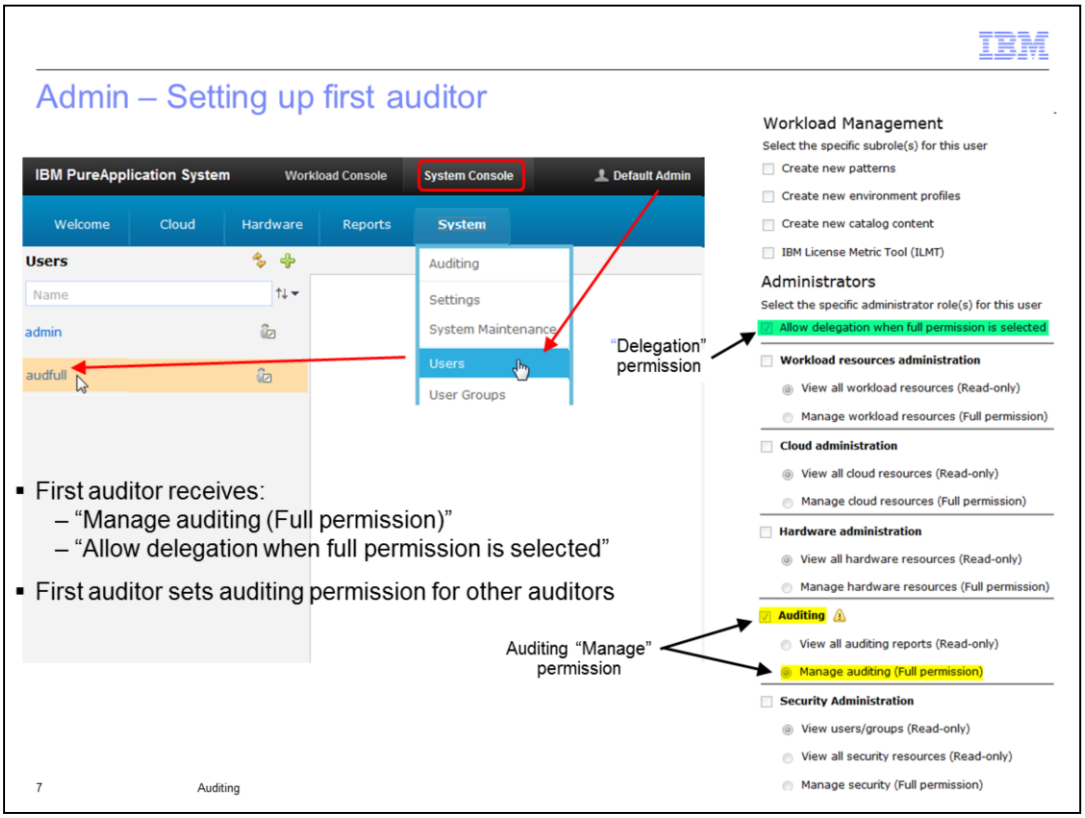
Creating users for auditing

- **System Console > System > Users > +**
  - The first administrator user or your Security administrator must create **all** user accounts for the auditor role
  - The first admin user account is defined in the Genesis process



© 2012 IBM Corporation

User account creation is the same for auditors as for any other user. If it is done using the administrative console, the first admin user or any administrator with permission to create user accounts can create the first auditor account. The example shows the first admin user account creating the first auditor.



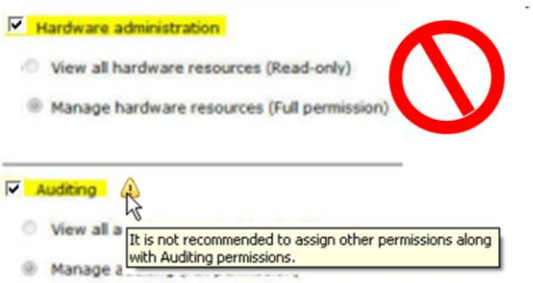
As part of the separation of duties, the first admin user account should set the permission for the first auditor with two permissions. The first auditor should receive "Manage auditing (Full permission)" and "Allow delegation when full permission is selected". It is not recommended, but there is nothing stopping the first admin user account from setting multiple auditors with either full or read-only permission. The recommendation is that the first auditor with full permission and with "Delegation" permission should manage the setting of permission of any other user accounts that are potential auditors.

Note that an auditor user cannot reset their own permissions. Another auditor with Delegation permission - or less desirably the administrator - must reset the auditing permission.

Like all other users, an auditor inherits the ability to deploy patterns in the cloud, but deploying patterns is not the intended role of an auditor.

Warning when mixing roles

- PureApplication System provides guidance when assigning permissions
- Auditing permission should not be mixed with other permissions
  - Exception: Allowing “Delegation” permission is within best practices

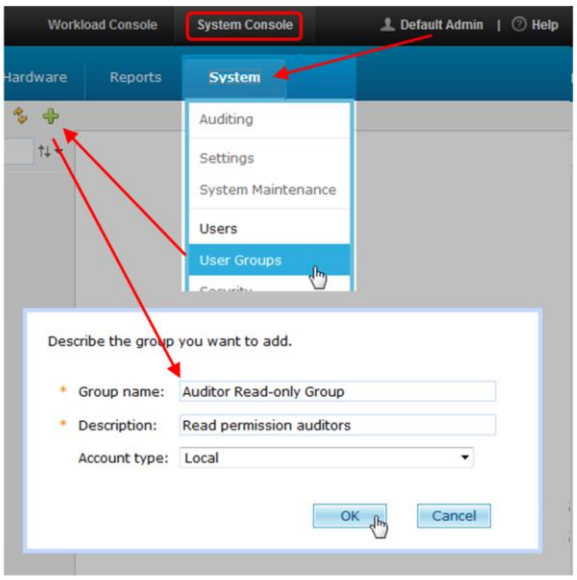


© 2012 IBM Corporation

Except for “Delegation” permission, it is not recommended to give a user auditing permission along with any other permission. When either auditing permission “View” or “Manage” permission is set, a warning message displays, reminding you that you should not configure this user with any other permissions. The example shows a user configured with “Manage Auditing (Full permission)” along with “Hardware administration” permission, which is not recommended.

Creating auditor groups – administrator

- **System Console > System > User Groups > +**
- First admin user account or security user account creates groups that are to have auditor permission
  - Administrators still must add ALL auditor users to auditor groups
  - Auditor with full permission will then set permissions for group



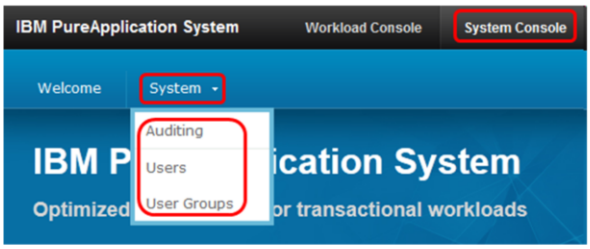
9 Auditing © 2012 IBM Corporation

Auditor group creation is similar to auditor user creation. All auditor groups must be created by the first admin user or Security administrator having full permission. The group that is to have auditing full or read-only permission is assigned their auditing permission by another auditor that has Full permission and Delegation permission. There is nothing stopping an administrator from setting the auditor group permissions, but best practice prescribes that an auditor should set the auditing permission.

Note that only the first admin user account or Security administrator has the permission to add auditor users to auditor groups.

Auditing – full permission user

- Logged on to “audfull” user
- Primary functions
  - Managing auditing permission for users and groups; requires:
    - “Manage auditing (Full permission)”
    - “Delegation” permission
  - Review event log utilization
  - Download and review audit record packages
  - Configure External Storage Server
  - Download Command Line tools
  - Generate a new package



© 2012 IBM Corporation

When you log into the System Console for PureApplication System as an auditor with “Manage auditing (Full permission), the menu dynamically reflects your permissions. Under the System pull-down menu, you see the capabilities offered to the auditor with “Manage auditing (Full permission)” and “Delegation” permission. The primary function of this “Full permission” auditor is to manage auditing permission for other auditor users and for auditor groups and, additionally, to work with the auditing functions and record packages. The auditing capabilities include reviewing event log utilization, downloading and reviewing audit record packages, configuring the External Storage Server, downloading Command Line tools, and generating a new audit record package. You will learn more about Audit Record Packages and External Storage Server later.

Auditing – read-only user

- Logged on to “audread” user
- Read-only allows auditor to:
  - Review event log utilization
  - Download and review audit record packages
  - Download Command Line tools
  - Generate a new record package

© 2012 IBM Corporation

When you log into System Console for PureApplication System as an auditor with “View all auditing reports (Read-only)” permission, the System menu provides only the “Auditing” menu selection. The primary capabilities of the read-only auditor are to review event log utilization and to download and review specific audit record packages. Additionally, the auditor with “Read-only” permission can download Command Line tools and generate a new audit record package. Unlike the auditor with full permission, the read-only auditor cannot review user or group permissions, cannot set auditing permission on or off, and can review but not configure the External Storage Server settings.

Section

Auditing functions

© 2012 IBM Corporation

This section discusses the auditing functions.

What is audited

- User activity, security events, and configuration changes within PureApplication System and in the cloud
- Audit record package do not include license and PVU data
- Format of downloaded audit record package
  - Different format than IBM Workload Deployer V3.1 auditing archives

© 2012 IBM Corporation

Unlike IBM Workload Deployer V3.1, which included the auditing archive, license information and pvu information in the same download, PureApplication System includes only auditing information from the archiving facility. The license-audit and pvu-audit information is available using a different facility, and the auditor cannot access this information.

The record format for the PureApplication System audit record package is different from auditing archives in IBM Workload Deployer V3.1.

What is auditing – more detail

- **User activity on the system**
  - Success or failure of login attempts
  - User (creation, deletion or update)
  - User group (creation, deletion or update)
  - Every user permission assignment
  - Configuration changes
  - Session timeout
  - Backup profile (creation, deletion or update)
  - IBM CE operations

- **User activity on cloud objects and data**
  - Security violation
  - Success or failure of attempts to access a security file or protected resource
    - Note: To provide context about these attempts, PureApplication System records provide details about the protected file or resources and users who can access them
  - Session timeout
  - Granting and ungranting users or groups
  - Plugins (creation, deletion or update)
  - Pattern types (creation, deletion or update)
  - Certificates (creation, deletion or update)
  - Success or failure of access attempts to Shared services
  - Success or failure of access attempts to virtual machines

© 2012 IBM Corporation

Click Stop on your player if you want to read the details on this slide that show the types of events for which audit records are written. Each Audit Record Package contains detail records, which contain information about activities listed on this chart. Details within the records provide information about the activity on the system and activity on cloud objects and data.

System Console > System > Auditing

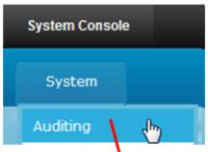
- General Status
  - Database utilization
- Audit Record Packages
  - Download using your browser
- External Storage Server (optional)
  - Any auditor can review
  - Only "Full permission" auditor can configure
    - Section must be completed for automatic "push" of audit record packages to external storage server

15 Auditing © 2012 IBM Corporation

This slide shows the primary three functions an auditor can perform in regard to the auditing data collected on PureApplication System.

The auditor can review the auditing database usage. The auditor can download and review Audit Record Packages. Additionally, an auditor with full permission can configure an External Storage Server so PureApplication System can automatically move Audit Record Packages to an external SCP server. However, an auditor with "Read-only" permission can only see the settings for the External Storage Server but cannot change any of the settings.

System Console > System > Auditing – General Status



General Status

Current event log utilization 74%

Shows event buffer utilization
- Click **Refresh** icon to see updated value

16 Auditing © 2012 IBM Corporation

General Status provides the current utilization of the auditing database, 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** icon to see a refreshed value.

System Console > System > Auditing – Audit Record Packages

- Existing Audit Record Packages in PureApplication System available for download
  - Available until space is reclaimed
- Generate a new Audit Record Package
  - Package is added to the list of packages
- Minimum time item stays on this list: 16 minutes

Audit Record Packages

Generate a new audit log package

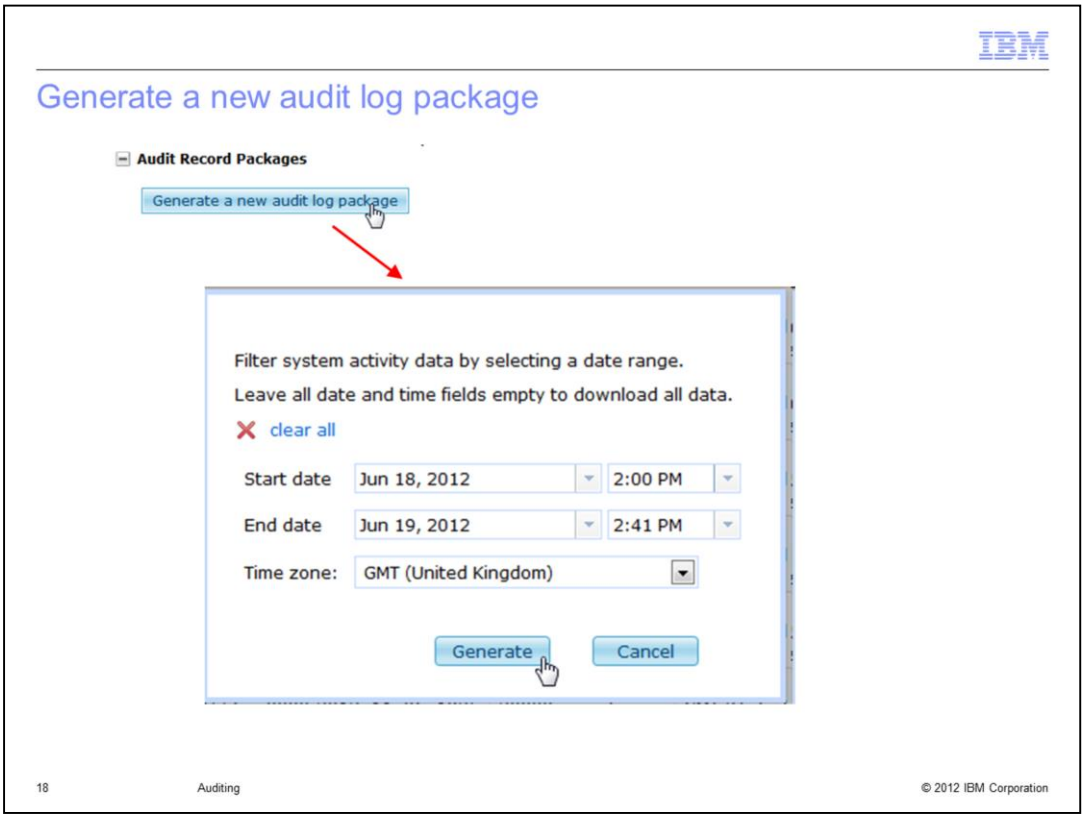
Created On	File Name	Size	Timezone	State	Action
7/6/12 6:15 AM GMT	puresystems-auto-audit-2012_05_07_184618_GMT-2012_06_07_042041_GMT.csv.gz	20000 records	GMT (United Kingdom)	Available	
7/6/12 4:29 AM GMT	puresystems-auto-audit-2012_05_07_061909_GMT-2012_05_07_221544_GMT.csv.gz	20000 records	GMT (United Kingdom)	Available	
7/5/12 10:30 PM GMT	puresystems-auto-audit-2012_04_07_144906_GMT-2012_05_07_182921_GMT.csv.gz	20000 records	GMT (United Kingdom)	Available	
7/5/12 6:55 PM GMT	puresystems-auto-audit-2012_03_07_211721_GMT-2012_05_07_060936_GMT.csv.gz	20000 records	GMT (United Kingdom)	Available	
7/5/12 6:13 AM GMT	puresystems-auto-audit-2012_02_07_110921_GMT-2012_04_07_141109_GMT.csv.gz	20000 records	GMT (United Kingdom)	Available	
7/4/12 2:15 PM GMT	puresystems-auto-audit-2012_29_06_075139_GMT-2012_03_07_203008_GMT.csv.gz	20000 records	GMT (United Kingdom)	Available	
7/3/12 8:36 PM GMT	puresystems-auto-audit-2012_28_06_230956_GMT-2012_02_07_074030_GMT.csv.gz	20000 records	GMT (United Kingdom)	Available	
7/2/12 7:44 AM GMT	puresystems-auto-audit-2012_27_06_122453_GMT-2012_29_06_073626_GMT.csv.gz	20000 records	GMT (United Kingdom)	Available	

1 - 8 of 32 items 1 2 3 4

17 Auditing © 2012 IBM Corporation

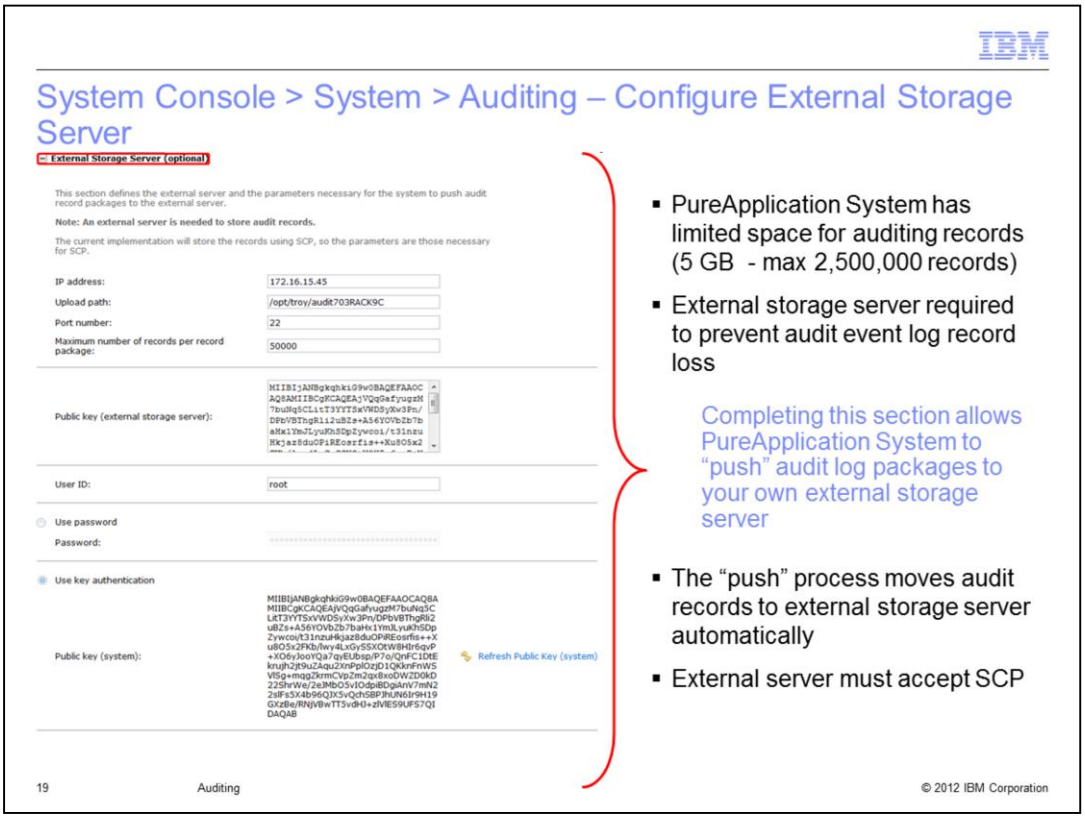
Here is an example of audit record packages that have been generated which are available for download by an auditor. The column headers indicate the **Created On** date, the **File Name** of the record package, and the **Size** of the record package by number of records. Note that the file name indicates the date and time range and time zone. The **Timezone** column shows the time zone for the generated record package. The **State** column shows the status of the request. The **Action** column provides a “download” link when the package is in the “Available” state. If you want to generate a new record, use the **Generate a new audit log package** link, described in a subsequent slide. By clicking the **Download** link, you can download the “Available” record packages.

If you don’t download an audit record package right away, the package will remain on the PureApplication System file system until space is reclaimed by PureApplication System. If you record the package ID, you can return to the **Existing Audit Record Packages** section of the auditing screen and click **Refresh**. Locate the log package you previously requested and click the download link at the right to download it. If the package is not there, generate the audit record package for the date/time range again. Records will remain in this list for a minimum time of 16 minutes.

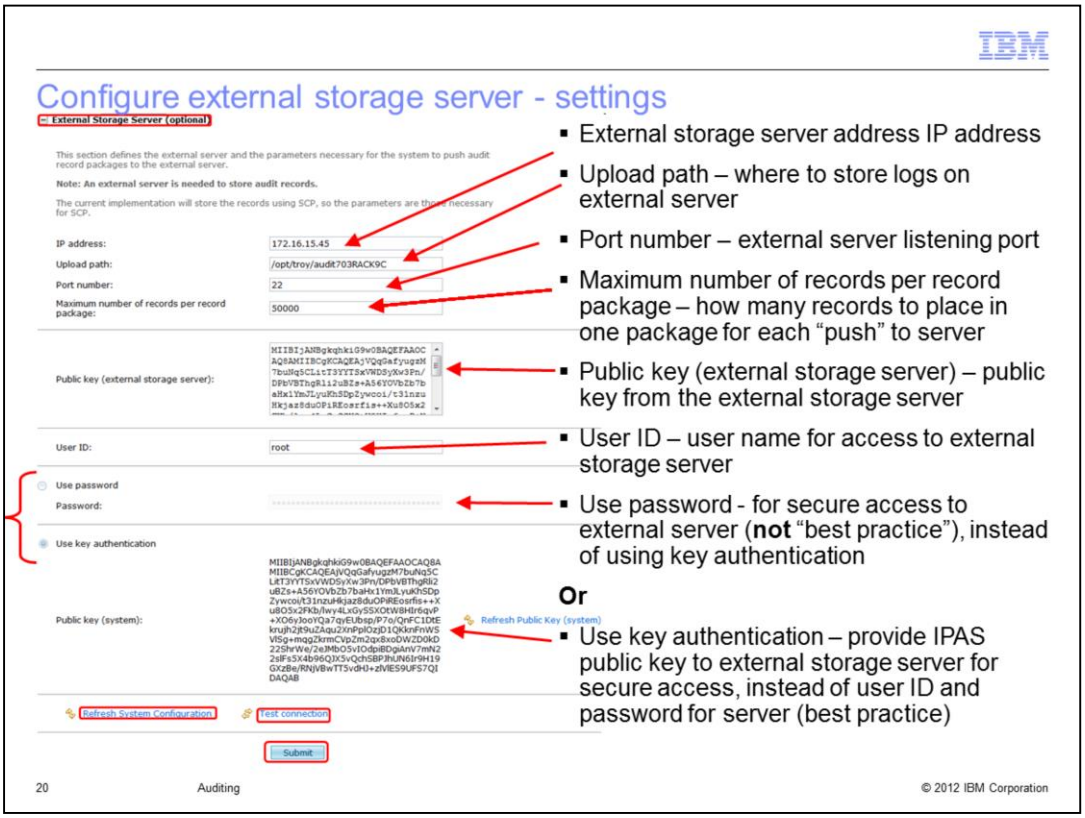


To generate an audit record package, click **Generate a new audit log package.** A window displays to allow you to type your filter data. In the **Start date** dropdown menu, you select the beginning date range for the audit record package. To the right is a time dropdown menu. If you do not select a beginning time, the package content will begin with the first available record on that date. In the **End date** dropdown menu, you selected the end date range for the audit record package. To the right is a time dropdown menu. If you do not select an end time, the package will end with the last available record on that date. The time zone field allows you to determine the time zone associated with your date and time filter requests. Click **Generate** to request the system to generate the log package.

Note that the time zone field affects the date and time range for the collection range. The time zone you specified is also reflected within the records in the audit record package you generated.



The PureApplication System has about five gigabytes of space in the internal database, so with an average record size of two kilobytes, the database will hold about two million five hundred thousand records. To prevent record loss in this database after it fills, you must configure an External Storage Server within PureApplication Server. This external server must accept SCP protocol. PureApplication Server then moves Audit Record Packages to this external server and then deletes the corresponding packages within the system and frees up internal disk space. Once you set up an External Storage Server, complete this screen and submit the changes to allow PureApplication Server to begin the "push" process. The next slide provides more details about this screen.



To activate the external storage server, complete all the required fields in the configuration.

In the URL field, provide the address of the external storage server.

Next, in the Upload path field, supply the file system path to the file location where you want PureApplication System to store the archived records.

In the Port number field, provide the listener port number for the external storage server.

In the Maximum number of records per record package field, supply the maximum number of records that you want in each package. The average size of an audit event record is approximately two kilobytes, so the specification of the field affects the average maximum size of the archived packages sent to the external storage server.

In the Public key (external storage server) field, you can paste public key you retrieve from the user account on your external storage server. If your security environment requires it, this key is provided to the external storage server so it can authenticate the PureApplication System. This field should not be completed if your external storage server does not require it.

In the User ID field, type the user name associated with the account on the external storage server.

In the next section, you can choose how PureApplication System authenticates the external storage server, depending on your environment. If security for your external storage server requires only a user ID and password, type the password for the external storage server account into the Password field and select the button next to Use password.

If you want to configure security so that the PureApplication Server authenticates the external server – which is a "Best Practice" recommendation - then click the radio button next to Use key authentication. The generated IPAS public key is then available for you to copy, so you can store it in your external storage server to allow IPAS to authenticate the external storage server and connect to it.

.

At the bottom left, you can click the Refresh System Configuration link to replace the values in this section of the screen which you might have overtyped with the values which are currently stored. You can click Test connection to see if your external server connection settings are valid. Once the fields are all correct, click Submit to store the values you have typed in this portion of the screen and to begin the "push" process.

Section

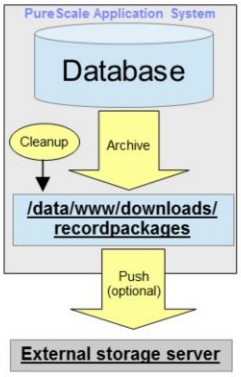
Management of audit records

© 2012 IBM Corporation

This section discusses the management of audit records.

Functions that manage audit records

- Archive (Archive)
  - Converts audit records from database to "Audit Record Packages"
  - Makes Audit Record Packages available for download
- Push (optionally configured) (Push (optional))
  - Moves Audit Record Packages to External Storage Server
- Cleanup (Cleanup)
  - Permanently deletes Audit Record Packages from PureApplication Server storage

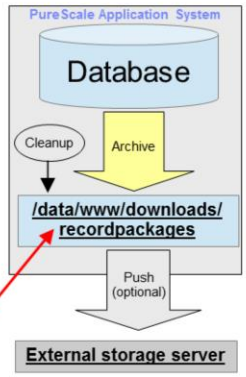


© 2012 IBM Corporation

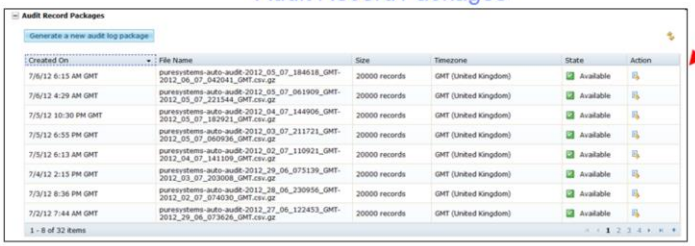
There are three functions that manage audit records in PureApplication System, indicated by the yellow arrows and circle. The **Archive** function converts the audit log event records in the system database into Audit Log Packages that you can download. If you have configured the External Storage Server in the auditing menu, the **Push** function sends the Audit Log Packages to your external storage server and deletes the associated Audit Record Package. The **Cleanup** function deletes the oldest "eligible" Audit Record Packages if space is needed for new audit record packages. The next slides show you more detail about each function.

Archive (manual or automatic)

- Creates the audit record package
  - Exports audit records from database
  - Creates a .csv file
  - Compresses it
- Places record package on Audit Record Package list
  - Downloadable from administrative console

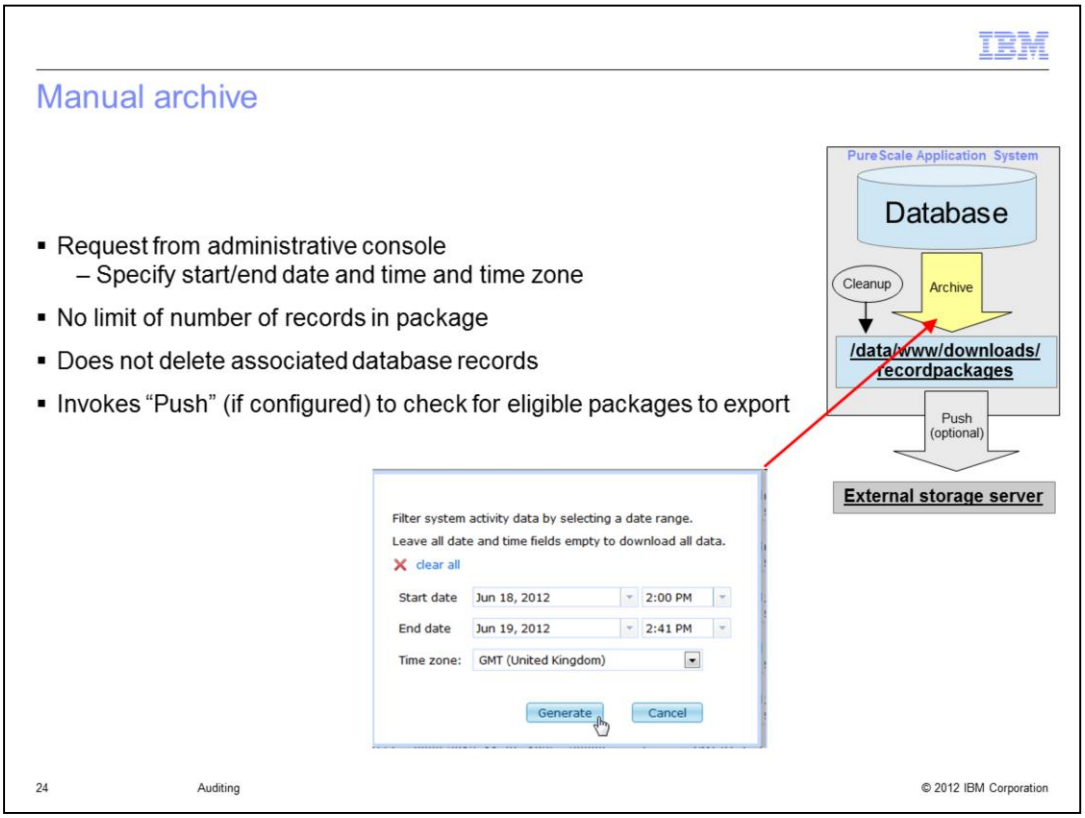


Audit Record Packages



23 Auditing © 2012 IBM Corporation

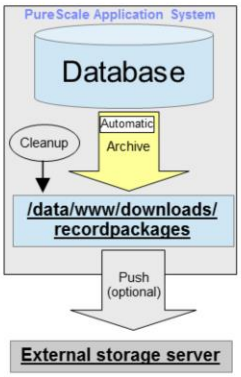
The **Archive** function creates the Audit Record Package. It exports the audit log event records from the database, creates a comma-separated-value file, and then compresses the file. The file is then made available for download on the Audit Record Package screen in the Auditing menu system on the administrative console. There are two types of **Archive** functions – manual and automatic - which you will learn about in the next few slides.



The **Manual Archive** function is initiated when you click **Generate a new audit log package** within the Audit Record Package menu. When the link is clicked, you see a popup window where you specify the time and date range and time zone for the records you want to see. You then click "Generate", which causes the archive function to create your requested Audit Record Package. You can download your requested Audit Record Package from the list of packages available within the administrative console. The associated database records are not deleted by the Manual Archive request. If the External Storage Server is configured, the "Push" process – discussed later in this presentation - is invoked to check for eligible packages to move to an external server.

Automatic archive

- Always available
- Monitors database every three minutes for record threshold
- Creates record package when threshold reached
- Uses External Storage Server setting for maximum number of records per package, if specified
  - Defaults to 20,000
- Starts with oldest records when creating package
- Deletes records from the database once package is created
- Invokes "Push" (if configured) to check for eligible packages to export

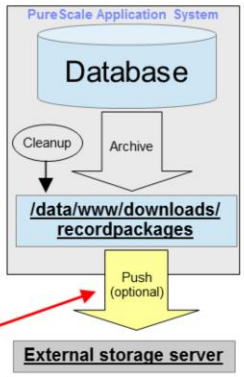


© 2012 IBM Corporation

The **Automatic archive** function is a background task that is always available on PureApplication Server, regardless of your configuration settings. The task monitors the database every three minutes. When a certain configurable record threshold is reached, **Automatic archive** will create a Audit Record Package – starting with the oldest database record. The package is added to the **Audit Record Packages** list in the administrative console for an auditor to download. Once the Audit Record Package is made available in the list, the associated database base records are deleted. If the External Storage Server is configured, the "Push" process is invoked to check for eligible packages to move to the external server.

Push

- Moves the archived Audit Record Packages to your external SCP server
  - Requires External Storage Server configuration
  - Begins with the oldest eligible Audit Record Package
  - Eligible package must be older than 1000 seconds (about 16 minutes)
    - Allows time for manual downloads
- Deletes the package when successfully transferred to the external storage server



External Storage Server screen

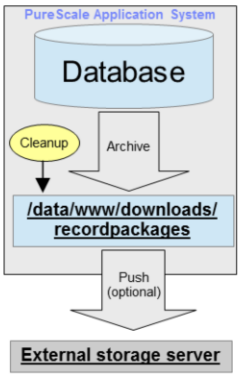
26 Auditing © 2012 IBM Corporation

If you configured the **External Storage Server** within the Auditing menu system, the **Push** function is available. This function moves the Audit Record Packages to an external SCP server that you define. The **Push** function starts with the oldest eligible packages within the **Audit Record Package** list. Note that any audit record package must be older than 1000 seconds - about 16 minutes - before it can be selected by **Push.** Once the selected package is delivered to the external storage server, the package is removed from the **Audit Record Package** list and deleted. If the external storage server is running and efficiently tuned, these record packages might only exist within the **Audit Record Package** list for about sixteen minutes before they are moved to the external storage server and deleted. During the time a package exists in the list, you can manually download the record package from the list.

If the external storage server rejects an auditing package, the package will remain in the **Audit Record Packages** list until the external storage server successfully stores it. If packages accumulate for a long period of time within PureApplication Server, eventually the **Cleanup** function will begin deleting the oldest eligible record packages as space is needed for newer packages. You learn more about **Cleanup** in the next slide.

Cleanup

- Deletes oldest record packages if space is needed for new record packages
  - Selects oldest eligible record package for deletion
    - Eligible package must be older than minimum age
      - 1000 seconds minimum age (about 16 minutes)
  - Continues deletion from oldest to newer until sufficient space is available for new record packages
- Can cause you to lose audit data
  - If External Storage Server is not configured
  - If External Storage Server is configured but becomes unavailable



© 2012 IBM Corporation

As previously indicated, only the **Push** function (optionally configured) and the **Cleanup** function can delete audit record packages. The **Cleanup** function is called when insufficient space exists to store new audit record packages. The function selects the oldest eligible record packages for deletion. This selection is made regardless of whether the package was generated by the manual archive process or by the automatic archive process. The oldest eligible packages are deleted until sufficient space is made available for the new record package. Thus you can lose audit data if an external storage server is not configured or if the external storage server becomes unavailable for a sufficient period of time for the audit record package file system to become full.

Summary of auditing functions

External Storage Server Configured?	Archive		Push	Cleanup	Download packages from administrative console
	Manual	Automatic			
No	✓	✓		✓	✓
Yes	✓	✓	✓	✓	✓

© 2012 IBM Corporation

Here is a summary of the functions available on PureApplication Server, based on whether you have configured the External Storage Server. Notice that Automatic Archive function continues to automatically archive database records to Audit Record Packages, regardless of your External Storage Server settings.

Auditing record management summary

- Database records
  - Cannot be “directly” deleted
  - Are periodically processed by “Archive” process
- Audit Record Packages
  - Cannot be “directly” deleted
  - Managed by **Push** and **Cleanup** functions
  - **Push** stores the records on the External Storage Server you defined
  - **Push** can be “inactive” if:
    - You did not configure External Storage Server, **or**
    - You configured External Storage Server but external server rejects **Push** requests
- You can lose Audit Record Packages if **Push** is not active
  - Package file system will eventually become full
    - **Automatic** and **Manual Archive** still active
      - New packages continue to be created
    - **Cleanup** function will begin to delete oldest eligible record packages to make room for new record packages
    - You can download from **Audit Record Packages** list

29 Auditing © 2012 IBM Corporation

Audit database records cannot be deleted by an auditor. The system removes database records when the automatic archive function runs.

Audit Record Package management is performed by either **Push** function, which stores the record packages on an external server, or by **Cleanup** functions. **Push** can be inactive if you never configured the External Storage Server, or if your External Storage Server cannot accept the record packages from PureApplication Server. In that situation the package file system will eventually becomes full, but **Automatic** and **Manual Archive** functions still function, thus creating new packages. When a new Audit Record Package needs to be written in this situation, **Cleanup** is called to create the needed space by deleting the oldest eligible packages. Thus, in this situation you can lost Audit Record Packages if you have not previously downloaded them.

During the time when the file system is full, you can still download packages from the **Audit Record Package** list in the administrative console.

External storage server considerations

- External storage server must have:
  - Security appropriate for your environment
  - Support for SCP – choose RSA key or UserID and Password
    - RSA keys
      - Best practice and recommended for maximum security
    - Password access
      - Less secure than RSA key
  - Prevent your external storage sever file system from becoming full
    - Permanently archive record packages on External Storage Server
    - If External Storage Server file system becomes full
      - PureApplication System will begin filling up its own file system to store audit records package files
      - If the file system in PureApplication System becomes full you can lose audit record packages

© 2012 IBM Corporation

Your external storage server must have security appropriate for your environment. It must have support for SCP with security implemented by RSA keys, which is best practice, or password. You must have an archiving system or a process to keep the file system on the External Storage Server from becoming full, to avoid the loss of Audit Record Packages on PureApplication System.

Section

Summary

© 2012 IBM Corporation

This section provides a summary of the presentation.

Summary

- Separation of duties
- Assigning users to the auditing role
- Auditing functions
- Management of audit records

© 2012 IBM Corporation

You now should understand the importance of separating the auditing and PureApplication System administration duties. You saw how the auditor user accounts are created and how they acquire the necessary permissions. A summary of the enhanced auditing functionality showed you important auditing features available in PureApplication System. Finally you saw more information about the management of audit records.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, PureApplication Server and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

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.

© Copyright International Business Machines Corporation 2012. All rights reserved.

© 2012 IBM Corporation