How to Integrate ServiceNow Ticketing with Policy-based Privilege Authorization in PowerBroker for Unix & Linux

Walk-through Guide

This brief guide has been prepared to illustrate the steps involved in configuring PowerBroker for Unix & Linux to work with ServiceNow to create, validate, elevate and update tickets directly at the Unix/Linux command line.

Use Cases

We have created walk-through videos of the following use cases:

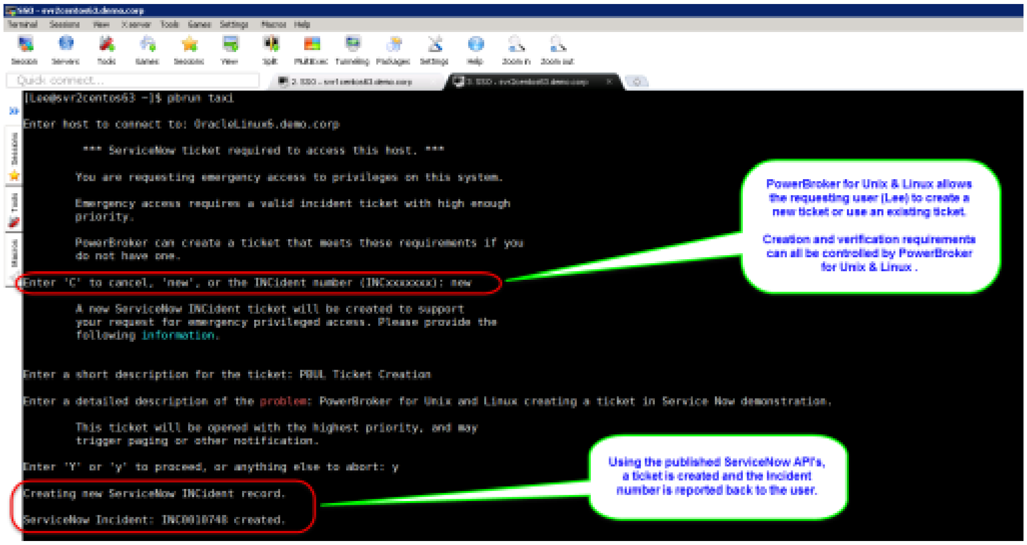
- Creating a ServiceNow ticket from the Unix/Linux command line
- Validating a ServiceNow ticket in order to elevate a user's permissions
- Updating a ServiceNow ticket from the Unix/Linux command line

This guide will provide a step-by step narrative to accompany these videos.

Creating a ServiceNow Ticket Through a Jump Host Connection

Description: A non-privileged user requesting access to another server (Jump Host) and creating a ticket in ServiceNow from within a Unix/Linux terminal session.

1) A non-privileged user (Lee the Unix admin) with a standard terminal session.
2) Lee is asked to investigate an issue on an Oracle database server.
3) Lee initiates a request (Jump Host connection) to the problematic server.
4) In order to connect, Lee creates a ServiceNow ticket during the Jump Host request.
5) Lee must provide requested details for the ticket.
6) Access and all associated details are documented within the ServiceNow ticket.
7) PowerBroker for Unix & Linux must also authorize access and then establish the remote session.

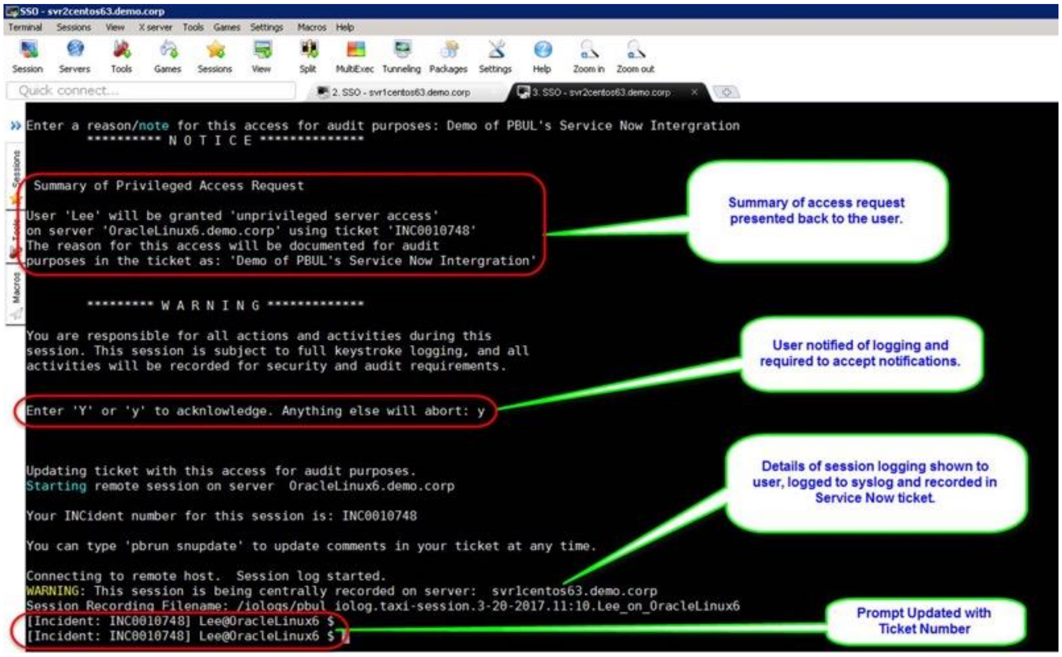

SSO - svr2centos63.demo.corp
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help Zoom in Zoom out
Quick connect...
2. SSO - svr1centos63.demo.corp
3. SSO - svr2centos63.demo.corp

```
[Lee@svr2centos63 ~]$ pbrun taxi

Enter host to connect to: OracleLinux6.demo.corp

        *** ServiceNow ticket required to access this host. ***

       You are requesting emergency access to privileges on this system.

       Emergency access requires a valid incident ticket with high enough
       priority.

       PowerBroker can create a ticket that meets these requirements if you
       do not have one.

Enter 'C' to cancel, 'new', or the INCident number (INCxxxxxxx): new

       A new ServiceNow INCident ticket will be created to support
       your request for emergency privileged access. Please provide the
       following information.


Enter a short description for the ticket: PBUL Ticket Creation

Enter a detailed description of the problem: PowerBroker for Unix and Linux creating a ticket in Service Now demonstration.

       This ticket will be opened with the highest priority, and may
       trigger paging or other notification.

Enter 'Y' or 'y' to proceed, or anything else to abort: y

Creating new ServiceNow INCident record.

ServiceNow Incident: INC0010748 created.
```

PowerBroker for Unix & Linux allows the requesting user (Lee) to create a new ticket or use an existing ticket.

Creation and verification requirements can all be controlled by PowerBroker for Unix & Linux .

Using the published ServiceNow API's, a ticket is created and the incident number is reported back to the user.


SSO - svr2centos63.demo.corp
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help Zoom in Zoom out
Quick connect...
2. SSO - svr1centos63.demo.corp
3. SSO - svr2centos63.demo.corp

```
Enter a reason/note for this access for audit purposes: Demo of PBUL's Service Now Intergration
          ********** N O T I C E **************

 Summary of Privileged Access Request

User 'Lee' will be granted 'unprivileged server access'
on server 'OracleLinux6.demo.corp' using ticket 'INC0010748'
The reason for this access will be documented for audit
purposes in the ticket as: 'Demo of PBUL's Service Now Intergration'


          ********* W A R N I N G *************

You are responsible for all actions and activities during this
session. This session is subject to full keystroke logging, and all
activities will be recorded for security and audit requirements.

Enter 'Y' or 'y' to acknlowledge. Anything else will abort: y


Updating ticket with this access for audit purposes.
Starting remote session on server  OracleLinux6.demo.corp

Your INCident number for this session is: INC0010748

You can type 'pbrun snupdate' to update comments in your ticket at any time.

Connecting to remote host.  Session log started.
WARNING: This session is being centrally recorded on server:  svrlcentos63.demo.corp
Session Recording Filename: /iologs/pbul iolog.taxi-session.3-20-2017.11:10.Lee_on_OracleLinux6
[Incident: INC0010748] Lee@OracleLinux6 $
[Incident: INC0010748] Lee@OracleLinux6 $
```

Summary of access request presented back to the user.

User notified of logging and required to accept notifications.

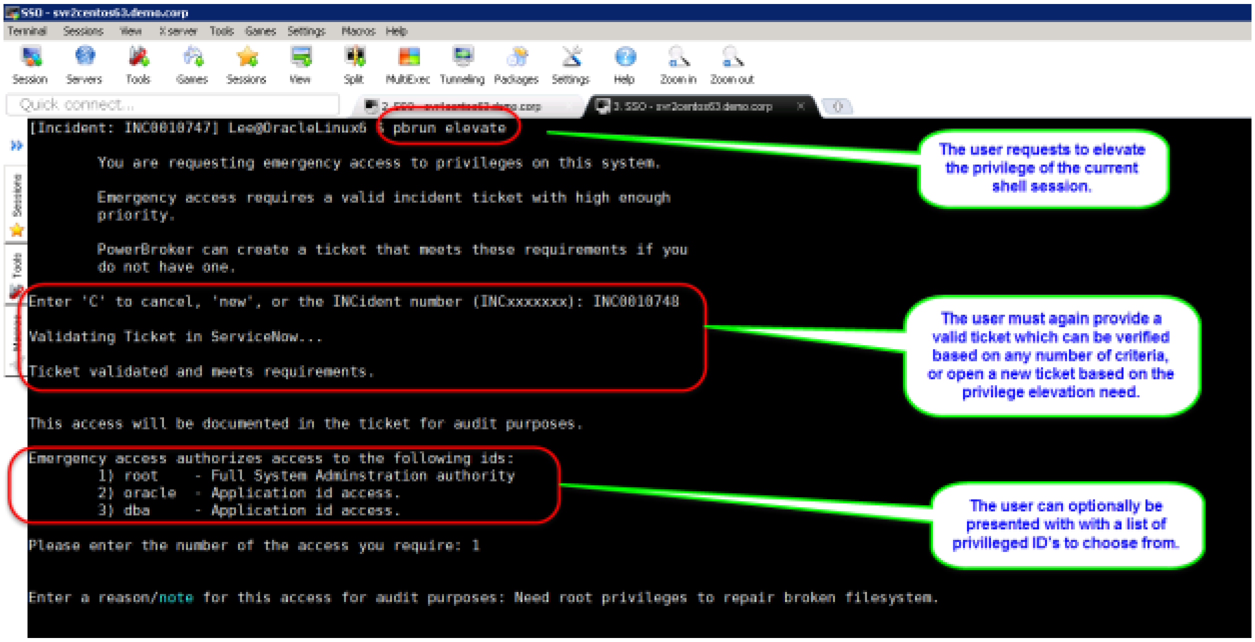
Details of session logging shown to user, logged to syslog and recorded in Service Now ticket.

Prompt Updated with Ticket Number

Elevating a Session with ServiceNow Validation

Description: A non-privileged user requesting elevated rights validated against an active ServiceNow ticket.

1) While working on the Oracle Database server, Lee requires elevated rights to fix the problem.
2) After requesting privilege elevation, Lee is required to enter a valid ServiceNow ticket.
3) The ticket is validated against ServiceNow (ticket number, priority and urgency are checked).
4) PowerBroker for Unix & Linux must also authorize the requested elevation.
5) The elevated session is initiated, session recording started and the ServiceNow ticket is updated with the request details, including the recorded session log filename.

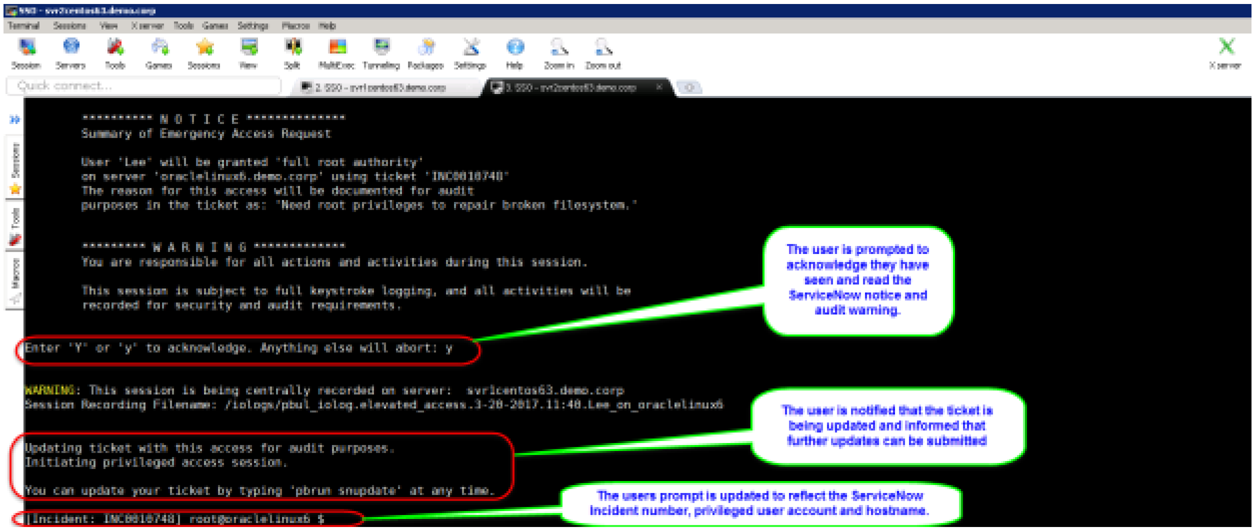

SSO - svr2centos63.demo.corp
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help Zoom in Zoom out
Quick connect...
2. SSO - svr1centos63.demo.corp
3. SSO - svr2centos63.demo.corp

```
[Incident: INC0010747] Lee@OracleLinux6 $ pbrun elevate

        You are requesting emergency access to privileges on this system.

        Emergency access requires a valid incident ticket with high enough
        priority.

        PowerBroker can create a ticket that meets these requirements if you
        do not have one.

Enter 'C' to cancel, 'new', or the INCident number (INCxxxxxxx): INC0010748

Validating Ticket in ServiceNow...

Ticket validated and meets requirements.

This access will be documented in the ticket for audit purposes.

Emergency access authorizes access to the following ids:
        1) root     - Full System Adminstration authority
        2) oracle   - Application id access.
        3) dba      - Application id access.

Please enter the number of the access you require: 1

Enter a reason/note for this access for audit purposes: Need root privileges to repair broken filesystem.
```

The user requests to elevate the privilege of the current shell session.

The user must again provide a valid ticket which can be verified based on any number of criteria, or open a new ticket based on the privilege elevation need.

The user can optionally be presented with with a list of privilleged ID's to choose from.


SSO - svr2centos63.demo.corp
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help Zoom in Zoom out
X server
Quick connect...
2. SSO - svr1centos63.demo.corp
3. SSO - svr2centos63.demo.corp

```
        ********** N O T I C E **************
        Summary of Emergency Access Request

        User 'Lee' will be granted 'full root authority'
        on server 'oraclelinux6.demo.corp' using ticket 'INC0010748'
        The reason for this access will be documented for audit
        purposes in the ticket as: 'Need root privileges to repair broken filesystem.'


        ********* W A R N I N G *************
        You are responsible for all actions and activities during this session.

        This session is subject to full keystroke logging, and all activities will be
        recorded for security and audit requirements.


Enter 'Y' or 'y' to acknowledge. Anything else will abort: y


WARNING: This session is being centrally recorded on server:  svr1centos63.demo.corp
Session Recording Filename: /iologs/pbul_iolog.elevated_access.3-20-2017.11:40.Lee_on_oraclelinux6


Updating ticket with this access for audit purposes.
Initiating privileged access session.

You can update your ticket by typing 'pbrun snupdate' at any time.

[Incident: INC0010748] root@oraclelinux6 $
```

The user is prompted to acknowledge they have seen and read the ServiceNow notice and audit warning.

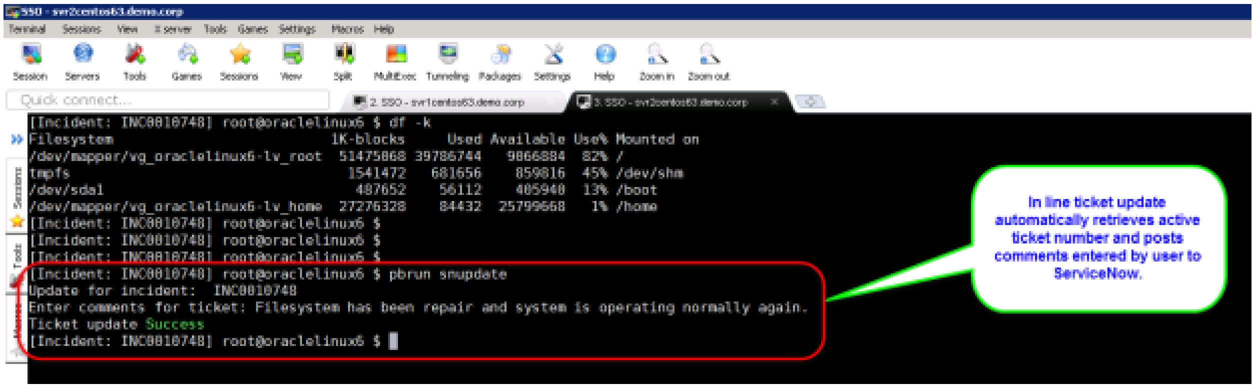
The user is notified that the ticket is being updated and informed that further updates can be submitted

The users prompt is updated to reflect the ServiceNow Incident number, privileged user account and hostname.

Updating a ServiceNow Ticket In-line

Description: ServiceNow ticket being updated from the Unix/Linux command line.

1) At any time while working the problem, or after resolving the problem, Lee wants to provide an update to the ServiceNow ticket.
2) A ticket update is initiated using the 'pbun snupdate' command.
3) Lee is prompted for a text update directly at the command line.
4) The ticket is updated without Lee leaving the terminal session.

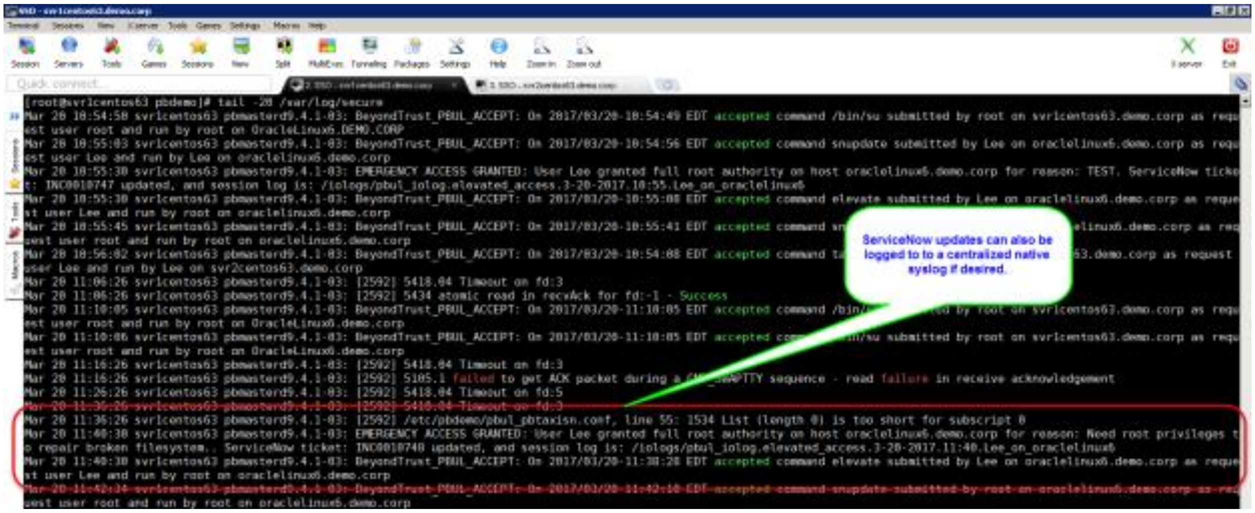


```
[Incident: INC0010748] root@oraclelinux6 $ df -k
Filesystem                         1K-blocks     Used Available Use% Mounted on
/dev/mapper/vg_oraclelinux6-lv_root  51475868 39786744   9066884  82% /
tmpfs                                 1541472   681656    859816  45% /dev/shm
/dev/sda1                              487652    56112    405940  13% /boot
/dev/mapper/vg_oraclelinux6-lv_home  27276328    84432  25799668   1% /home
[Incident: INC0010748] root@oraclelinux6 $
[Incident: INC0010748] root@oraclelinux6 $
[Incident: INC0010748] root@oraclelinux6 $
[Incident: INC0010748] root@oraclelinux6 $ pbrun snupdate
Update for incident:  INC0010748
Enter comments for ticket: Filesystem has been repair and system is operating normally again.
Ticket update Success
[Incident: INC0010748] root@oraclelinux6 $
```

SSO - svr2centos63.demo.corp
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help Zoom in Zoom out
Quick connect...
2. SSO - svr1centos63.demo.corp
3. SSO - svr2centos63.demo.corp
In line ticket update automatically retrieves active ticket number and posts comments entered by user to ServiceNow.

ServiceNow and SYSLOG

It is possible to update syslog with the same information that is being sent to ServiceNow in addition to the regular 'Eventlog' and optional 'Session Recordings' generated by PowerBroker for Unix & Linux:

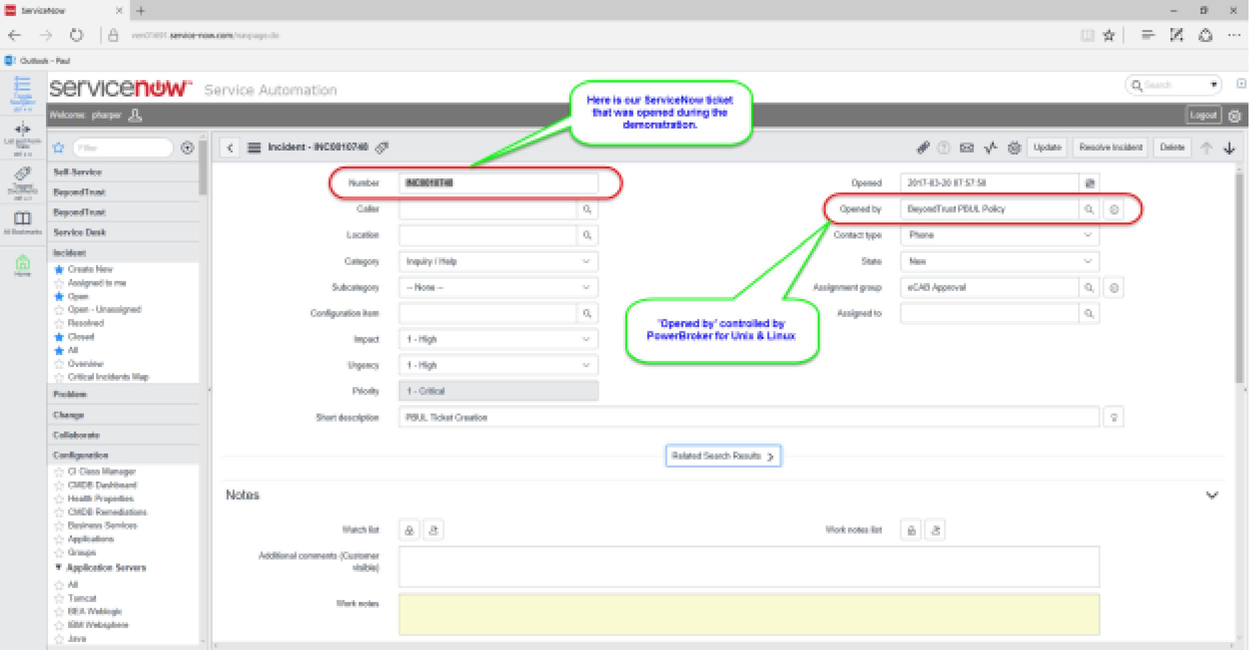


```
[root@svr1centos63 pbdemo]# tail -20 /var/log/secure
Mar 20 10:54:58 svr1centos63 pbmasterd9.4.1-03: BeyondTrust_PBUL_ACCEPT: On 2017/03/20-10:54:49 EDT accepted command /bin/su submitted by root on svr1centos63.demo.corp as requ
est user root and run by root on OracleLinux6.DEMO.CORP
Mar 20 10:55:03 svr1centos63 pbmasterd9.4.1-03: BeyondTrust_PBUL_ACCEPT: On 2017/03/20-10:54:56 EDT accepted command snupdate submitted by Lee on oraclelinux6.demo.corp as requ
est user Lee and run by Lee on oraclelinux6.demo.corp
Mar 20 10:55:30 svr1centos63 pbmasterd9.4.1-03: EMERGENCY ACCESS GRANTED: User Lee granted full root authority on host oraclelinux6.demo.corp for reason: TEST. ServiceNow ticke
t: INC0010747 updated, and session log is: /iologs/pbul_iolog.elevated_access.3-20-2017.10:55.Lee_on_oraclelinux6
Mar 20 10:55:30 svr1centos63 pbmasterd9.4.1-03: BeyondTrust_PBUL_ACCEPT: On 2017/03/20-10:55:08 EDT accepted command elevate submitted by Lee on oraclelinux6.demo.corp as reque
st user Lee and run by root on oraclelinux6.demo.corp
Mar 20 10:55:45 svr1centos63 pbmasterd9.4.1-03: BeyondTrust_PBUL_ACCEPT: On 2017/03/20-10:55:41 EDT accepted command sn                        elinux6.demo.corp as req
uest user root and run by root on oraclelinux6.demo.corp
Mar 20 10:56:02 svr1centos63 pbmasterd9.4.1-03: BeyondTrust_PBUL_ACCEPT: On 2017/03/20-10:54:08 EDT accepted command ta                        63.demo.corp as request
user Lee and run by Lee on svr2centos63.demo.corp
Mar 20 11:06:26 svr1centos63 pbmasterd9.4.1-03: [2592] 5418.04 Timeout on fd:3
Mar 20 11:06:26 svr1centos63 pbmasterd9.4.1-03: [2592] 5434 atomic read in recvAck for fd:-1 - Success
Mar 20 11:10:05 svr1centos63 pbmasterd9.4.1-03: BeyondTrust_PBUL_ACCEPT: On 2017/03/20-11:10:05 EDT accepted command /bin/        ed by root on svr1centos63.demo.corp as requ
est user root and run by root on OracleLinux6.demo.corp
Mar 20 11:10:06 svr1centos63 pbmasterd9.4.1-03: BeyondTrust_PBUL_ACCEPT: On 2017/03/20-11:10:05 EDT accepted co      in/su submitted by root on svr1centos63.demo.corp as requ
est user root and run by root on OracleLinux6.demo.corp
Mar 20 11:16:26 svr1centos63 pbmasterd9.4.1-03: [2592] 5418.04 Timeout on fd:3
Mar 20 11:16:26 svr1centos63 pbmasterd9.4.1-03: [2592] 5105.1 failed to get ACK packet during a CMD_SWAPTTY sequence - read failure in receive acknowledgement
Mar 20 11:26:26 svr1centos63 pbmasterd9.4.1-03: [2592] 5418.04 Timeout on fd:5
Mar 20 11:36:26 svr1centos63 pbmasterd9.4.1-03: [2592] 5418.04 Timeout on fd:3
Mar 20 11:36:26 svr1centos63 pbmasterd9.4.1-03: [2592] /etc/pbdemo/pbul_pbtaxisn.conf, line 55: 1534 List (length 0) is too short for subscript 0
Mar 20 11:40:30 svr1centos63 pbmasterd9.4.1-03: EMERGENCY ACCESS GRANTED: User Lee granted full root authority on host oraclelinux6.demo.corp for reason: Need root privileges t
o repair broken filesystem.. ServiceNow ticket: INC0010748 updated, and session log is: /iologs/pbul_iolog.elevated_access.3-20-2017.11:40.Lee_on_oraclelinux6
Mar 20 11:40:30 svr1centos63 pbmasterd9.4.1-03: BeyondTrust_PBUL_ACCEPT: On 2017/03/20-11:38:28 EDT accepted command elevate submitted by Lee on oraclelinux6.demo.corp as reque
st user Lee and run by root on oraclelinux6.demo.corp
Mar 20 11:42:34 svr1centos63 pbmasterd9.4.1-03: BeyondTrust_PBUL_ACCEPT: On 2017/03/20-11:42:10 EDT accepted command snupdate submitted by root on oraclelinux6.demo.corp as req
uest user root and run by root on oraclelinux6.demo.corp
```

SSO - svr1centos63.demo.corp
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help Zoom in Zoom out X server Exit
Quick connect...
2. SSO - svr1centos63.demo.corp
3. SSO - svr2centos63.demo.corp
ServiceNow updates can also be logged to to a centralized native syslog if desired.

ServiceNow Incident Web View

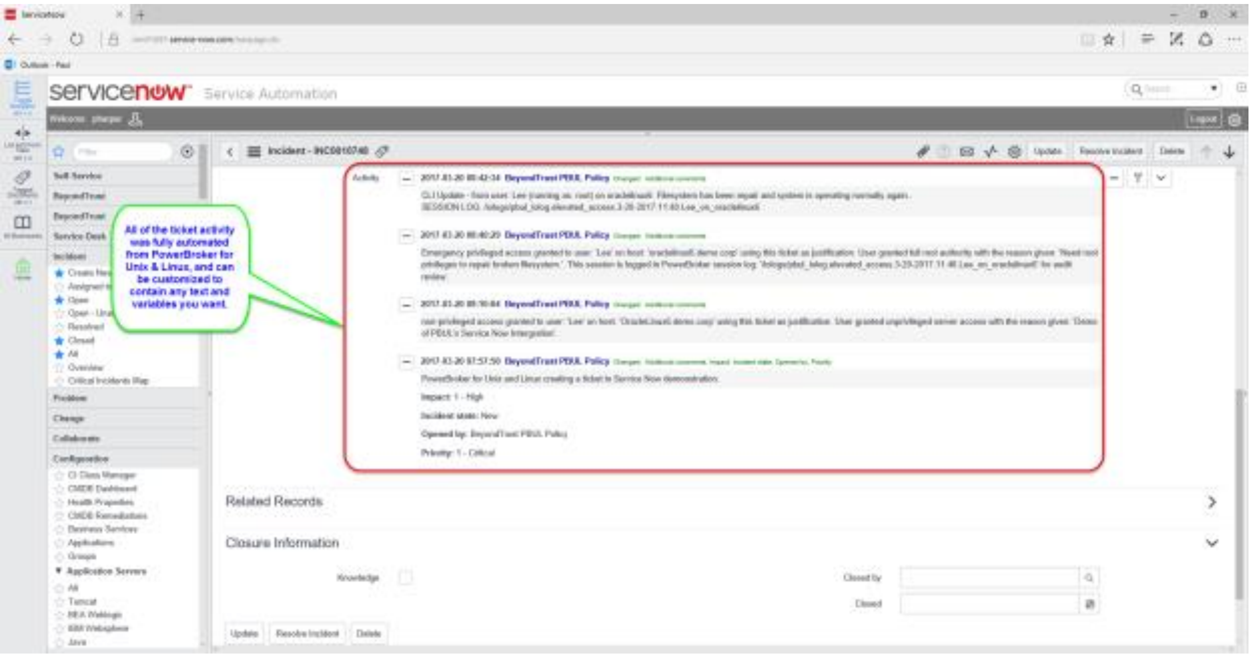
All of the activity from the user shell session are now fully logged into ServiceNow, including the justification comments made by the user and details of the associated session recording file which can be played back for a fully interactive view of what the user did and what the user saw during the session:



Here is our ServiceNow ticket that was opened during the demonstration.

'Opened by' controlled by PowerBroker for Unix & Linux

Number	INC0010740	Opened	2017-03-20 07:57:58
Caller		Opened by	BeyondTrust PBUL Policy
Location		Contact type	Phone
Category	Inquiry / Help	State	New
Subcategory	-- None --	Assignment group	eCAB Approval
Configuration item		Assigned to	
Impact	1 - High		
Urgency	1 - High		
Priority	1 - Critical		
Short description	PBUL Ticket Creation		



All of the ticket activity was fully automated from PowerBroker for Unix & Linux, and can be customized to contain any text and variables you want.

Activity

2017-03-20 08:42:34 BeyondTrust PBUL Policy Changed: Additional comments
CLI Update - from user: Lee (running as: root) on oracle8linux8. Filesystem has been repaired and system is operating normally again.
SESSION LOG: /iologs/pbul_iolog.elevated_access.3-20-2017.11:40.Lee_on_oracle8linux8

2017-03-20 08:40:20 BeyondTrust PBUL Policy Changed: Additional comments
Emergency privileged access granted to user: 'Lee' on host: 'oracle8linux8.demo.corp' using this ticket as justification. User granted full root authority with the reason given: 'Need root privileges to repair broken filesystem.' This session is logged in PowerBroker session log: '/iologs/pbul_iolog.elevated_access.3-20-2017.11:40.Lee_on_oracle8linux8' for audit review.

2017-03-20 08:10:04 BeyondTrust PBUL Policy Changed: Additional comments
non-privileged access granted to user: 'Lee' on host: 'OracleLinux8.demo.corp' using this ticket as justification. User granted unprivileged server access with the reason given: 'Demo of PBUL's Service Now Intergration'.

2017-03-20 07:57:50 BeyondTrust PBUL Policy Changed: Additional comments, Impact, Incident state, Opened by, Priority
PowerBroker for Unix and Linux creating a ticket in Service Now demonstration.
Impact: 1 - High
Incident state: New
Opened by: BeyondTrust PBUL Policy
Priority: 1 - Critical

About PowerBroker for Unix & Linux

PowerBroker for Unix & Linux is a least privilege solution that enables IT organizations to eliminate the sharing of credentials by delegating Unix and Linux privileges and elevating rights to run specific Unix and Linux commands without providing full root access. With complete auditing and recording of all user activity, a simple graphical user interface for management, and centralized policy management, organizations will more easily achieve their security and compliance objectives than with the limited functionality and vulnerability of tools such as sudo. PowerBroker enables organizations to:

- Elevate privileges on an as-needed basis, without exposing the root account password
- Monitor event logs and file integrity for unauthorized changes
- Capture keystrokes and screens with searchable playback for complete documentation of privileged user activity
- Simplify the management of all policies, roles and log data with a single point of administration
- Leverage a single least privilege enforcement solution across more than 100 flavors of Unix and Linux
- Achieve complete privilege management across all platforms – Windows, Mac, Unix and Linux

For more on PowerBroker for Unix & Linux, visit www.beyondtrust.com/products/powerbroker-for-unix-linux.