accenture

SAP ON CLOUD AUTOMATION

Secure Zero Trust Protection OSLogin+

July 2024

Dilemma – Human Error

Client # 1

During non-production **system refresh**, while performing prerequisite comparison checks between source and target systems, it was found that **production** system Database was accidentally SHUTDOWN due to which it went inaccessible…. .

→ **Controls on Critical/Restricted Commands at OS, DB & Applications**

Client # 2

Users belonging to SAP **Production** systems that were not in the Outage window were **locked** due to miscommunication between teams. As such multiple users could not login and a P1 was raised….

→ **Self-Awareness Visualization to be enhanced to avoid restriction of user access to systems**

Client # 3

Team member used non-production admin user account to assign **elevated access** for another active directory user….

→ **SUDO or equivalent Admin access to be controlled**

Accenture ZTP OSLogin+ - Why ZTP?

- **Business interruptions caused by unintended actions on servers**

  Internal Reviews and Root Cause Analysis identified prime reasons:

  - **Accidental human errors** due to oversight, miscommunication, or the rush of the moment.
  - Business team negotiates to implement **stringent downtime** policies.

- Mechanism is necessary to develop modules that could assist in minimizing accidental errors for practitioners handling critical activities.

- More importantly, need felt to implement restrictions for **Critical Commands** before they are executed at operating system level for OS, Database and application-specific activities.

Copyright © 2023 Accenture. All rights reserved.

What is ZTP OSLogin+?

ZTP OSLogin+ Package

The ZTP OSLogin+ Package helps the SAP Basis Administrator or a Linux Administrator to have awareness on what type of VM they connect to manage delivery tasks. When, in-rush of varied job-in-hand, one can accidentally assume a wrong terminal session and might execute command(s) or perform operations which is forbidden for that environment. This tool will minimize such risks and bring value to the administration team.

Software Licensing

- ✓ ZTP OSLogin+ Software will follow Server-Based Licensing model.
- ✓ ZTP OSLogin+ application can be used on TRIAL version for first 30 days beyond which projects needs to procure License on yearly basis. Maximum 100 user-ids per VM is allowed as of date.
- ✓ Requests for Customized addons / features which are client specific will be currently on hold from any modification
- ✓ Commercials are getting worked out now, and need to be discussed separately

What is ZTP OSLogin+? (Contd.)

What are the Pre-requisites?

1. Client InfoSec Team **Affirmation** to use the ZTP OSLogin+ software package on their environment.
2. A user with **root access** is required to install the tool.

NOTE: *Due to the varying AD user mechanisms, the tool must be tested thoroughly for AD users before using.*

How to Install the tool?

Detailed administrative manual available for interested clients.

Whom to contact for further queries?

Contact SAP-CloudCoE-CloudSuite@accenture.com for more details.

Accenture ZTP OSLogin+ - Features

ZTP OSLogin+ FEATURES

Login Package

Brings additional checks to validate Linux users and bring in controls for *Self-Awareness*

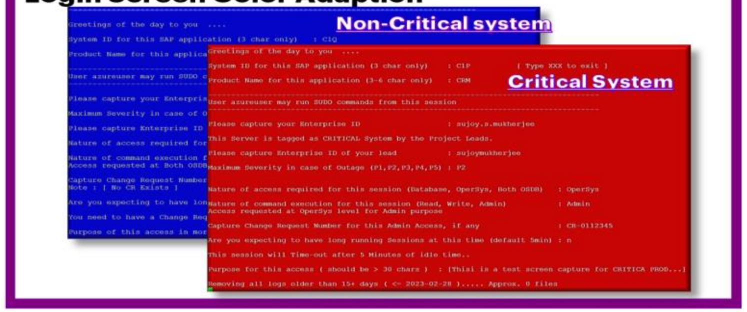
Prompt Package

Changes to the default prompt adds enhanced visualization with banner for Linux server identified as critical which brings in improved ALERT-ness

Command Package

Project specific critical OS Level commands can be Restricted based on server specific configurations

Login Screen Color Adaption

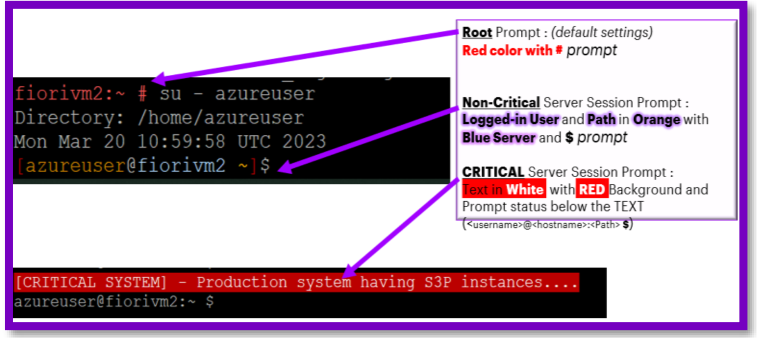


Non-Critical system

```
Greetings of the day to you  ....
System ID for this SAP application (3 char only)   : CIQ
Product Name for this applica
User azureuser may run SUDO c
Please capture your Enterpris
Maximum Severity in case of O
Please capture Enterprise ID
Nature of access required for
Nature of command execution f
Access requested at Both OSDB
Capture Change Request Number
Note : [ No CR Exists ]
Are you expecting to have lon
You need to have a Change Req
Purpose of this access in mor
```

Critical System

```
Greetings of the day to you  ....
System ID for this SAP application (3 char only)     : C1P         [ Type XXX to exit ]
Product Name for this application (3-6 char only)    : CRM
------------------------------------------------------------------------
User azureuser may run SUDO commands from this session
------------------------------------------------------------------------
Please capture your Enterprise ID                    : sujoy.s.mukherjee
This Server is tagged as CRITICAL System by the Project Leads.
Please capture Enterprise ID of your lead            : sujoymukherjee
Maximum Severity in case of Outage (P1,P2,P3,P4,P5) : P2

Nature of access required for this session (Database, OperSys, Both OSDB)    : OperSys
Nature of command execution for this session (Read, Write, Admin)            : Admin
Access requested at OperSys level for Admin purpose
Capture Change Request Number for this Admin Access, if any                  : CR-0112345
Are you expecting to have long running Sessions at this time (default 5min) : n
This session will Time-out after 5 Minutes of idle time..
Purpose for this access ( should be > 30 chars )  : [Thisi is a test screen capture for CRITICA PROD...]
Removing all logs older than 15+ days ( <= 2023-02-28 )..... Approx. 0 files
```



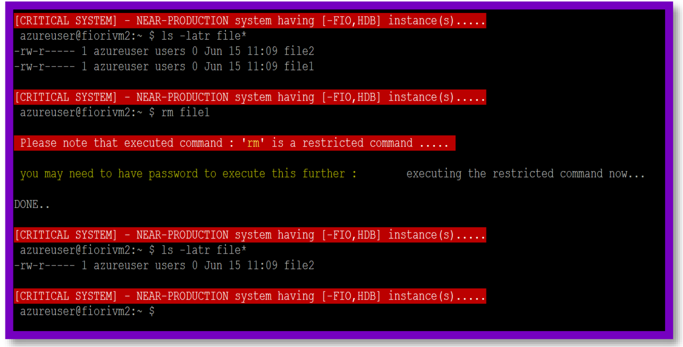
```
fiorivm2:~ # su - azureuser
Directory: /home/azureuser
Mon Mar 20 10:59:58 UTC 2023
[azureuser@fiorivm2 ~]$
```

```
[CRITICAL SYSTEM] - Production system having S3P instances....
azureuser@fiorivm2:~ $
```

Root Prompt : *(default settings)*
Red color with # *prompt*

Non-Critical Server Session Prompt :
Logged-in User and **Path** in **Orange** with **Blue Server** and **$** *prompt*

CRITICAL Server Session Prompt :
Text in **White** with **RED** Background and Prompt status below the TEXT
(<username>@<hostname>:<Path> **$**)



```
[CRITICAL SYSTEM] - NEAR-PRODUCTION system having [-FIO,HDB] instance(s).....
 azureuser@fiorivm2:~ $ ls -latr file*
-rw-r----- 1 azureuser users 0 Jun 15 11:09 file2
-rw-r----- 1 azureuser users 0 Jun 15 11:09 file1

[CRITICAL SYSTEM] - NEAR-PRODUCTION system having [-FIO,HDB] instance(s).....
 azureuser@fiorivm2:~ $ rm file1

 Please note that executed command : 'rm' is a restricted command .....

 you may need to have password to execute this further :       executing the restricted command now...

DONE..

[CRITICAL SYSTEM] - NEAR-PRODUCTION system having [-FIO,HDB] instance(s).....
 azureuser@fiorivm2:~ $ ls -latr file*
-rw-r----- 1 azureuser users 0 Jun 15 11:09 file2

[CRITICAL SYSTEM] - NEAR-PRODUCTION system having [-FIO,HDB] instance(s).....
 azureuser@fiorivm2:~ $
```

Be Self AWARE – *where are we login in…*

- Validate the Login with additional questions

Assist to stay Self ALERT – *Are we on right terminal…*

- Visualization of Change in the default Login Prompt Shell

Put Required CONTROL to encourage Best Practices

- Selective OS, Database and Application commands can now be defined as Restricted Commands

Who May Use	Who Can Not Use
All Linux users with local dedicated home directory and **enabled** to OSLogin+	Windows Based users. Tested for Linux (SLES,RHEL and OEL) only
Enabled Linux users who are on bash, Ksh or sh/zsh Shell environment	Login Package not applicable for Linux users with C-Shell* Environment.
	Linux users who are not enabled for ZTP OSlogin+

Copyright © 2023 Accenture. All rights reserved.

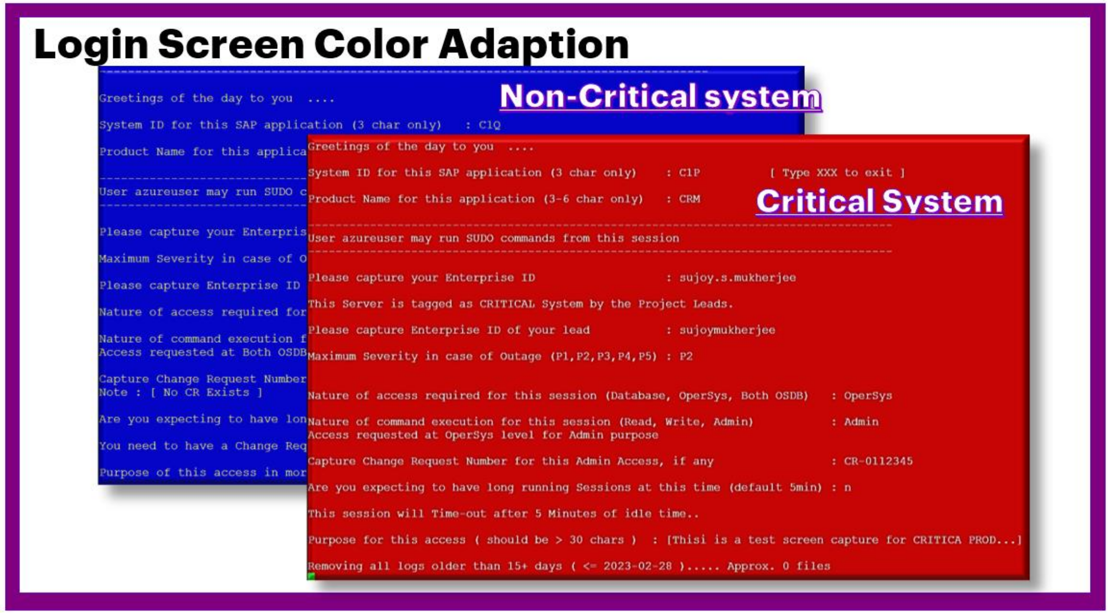
Challenges

- 4-Eye Review Principles
- LCR Pressure to Manage Workloads
- Unrestricted write access for Junior Practitioners

Solution

- **ZTP** OSLogin brings in enough controls that enables *Self-Awareness* and *Self-Alertness* to our Practitioners, while they are accessing SAP Operating systems / Servers.

Zero-Trust Validations



Login Screen Color Adaption

Non-Critical system

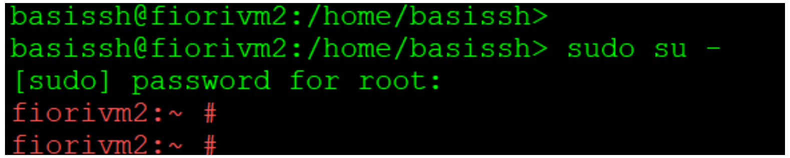
```
------------------------------------------------------------------------
Greetings of the day to you  ....
System ID for this SAP application (3 char only)    : C1Q
Product Name for this applica
------------------------------
User azureuser may run SUDO c
------------------------------
Please capture your Enterpris
Maximum Severity in case of O
Please capture Enterprise ID
Nature of access required for
Nature of command execution f
Access requested at Both OSDB
Capture Change Request Number
Note : [ No CR Exists ]
Are you expecting to have lon
You need to have a Change Req
Purpose of this access in mor
```

Critical System

```
Greetings of the day to you  ....
System ID for this SAP application (3 char only)    : C1P         [ Type XXX to exit ]
Product Name for this application (3-6 char only)   : CRM
-------------------------------------------------------------------------------------
User azureuser may run SUDO commands from this session
-------------------------------------------------------------------------------------
Please capture your Enterprise ID                   : sujoy.s.mukherjee
This Server is tagged as CRITICAL System by the Project Leads.
Please capture Enterprise ID of your lead           : sujoymukherjee
Maximum Severity in case of Outage (P1,P2,P3,P4,P5) : P2

Nature of access required for this session (Database, OperSys, Both OSDB)   : OperSys
Nature of command execution for this session (Read, Write, Admin)           : Admin
Access requested at OperSys level for Admin purpose
Capture Change Request Number for this Admin Access, if any                 : CR-0112345
Are you expecting to have long running Sessions at this time (default 5min) : n
This session will Time-out after 5 Minutes of idle time..
Purpose for this access ( should be > 30 chars )  : [Thisi is a test screen capture for CRITICA PROD...]
Removing all logs older than 15+ days ( <= 2023-02-28 )..... Approx. 0 files
```

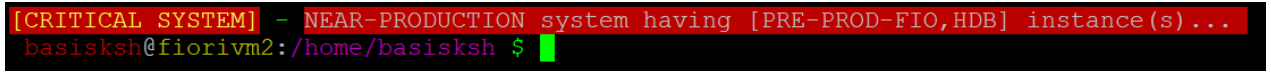
Visual Awareness – Re-defined Prompts

Default Prompts for **root** and **non-root** users without ZTP OSLogin enablement



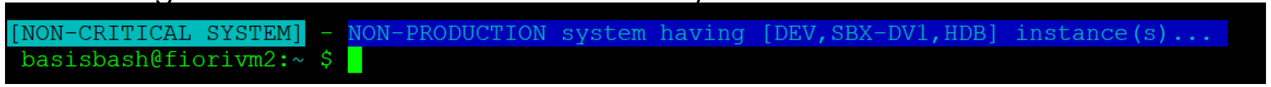
```
basissh@fiorivm2:/home/basissh>
basissh@fiorivm2:/home/basissh> sudo su -
[sudo] password for root:
fiorivm2:~ #
fiorivm2:~ #
```

ZTP OSLogin **Enabled** user on **Critical** system



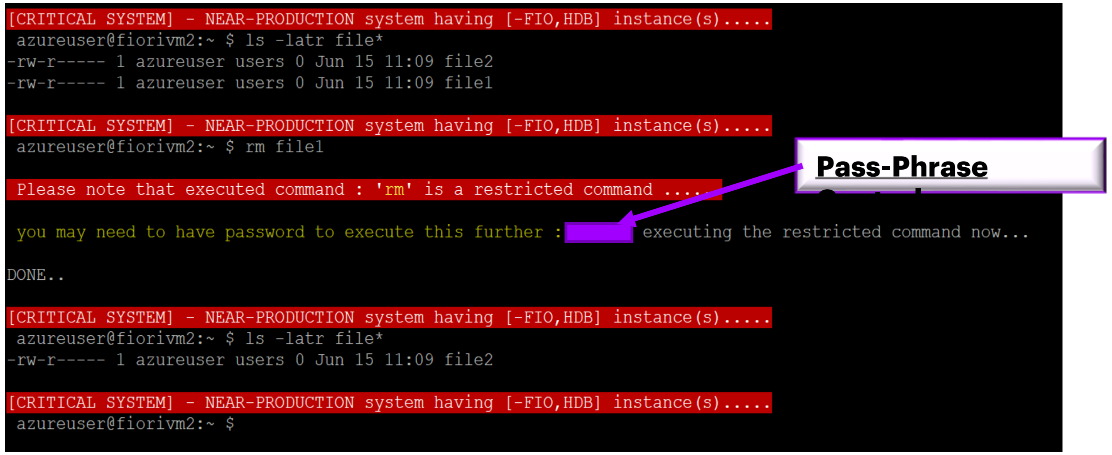
```
[CRITICAL SYSTEM] - NEAR-PRODUCTION system having [PRE-PROD-FIO,HDB] instance(s)...
 basisksh@fiorivm2:/home/basisksh $
```

ZTP OSLogin **Enabled** user on **Non-Critical** system



```
[NON-CRITICAL SYSTEM] - NON-PRODUCTION system having [DEV,SBX-DV1,HDB] instance(s)...
 basisbash@fiorivm2:~ $
```

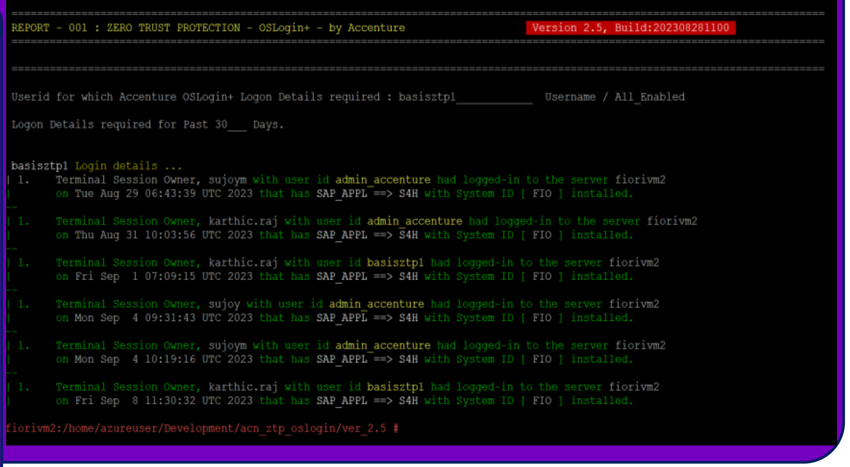
Enforced Protection for Critical /Restricted Commands



```
[CRITICAL SYSTEM] - NEAR-PRODUCTION system having [-FIO,HDB] instance(s).....
 azureuser@fiorivm2:~ $ ls -latr file*
-rw-r----- 1 azureuser users 0 Jun 15 11:09 file2
-rw-r----- 1 azureuser users 0 Jun 15 11:09 file1

[CRITICAL SYSTEM] - NEAR-PRODUCTION system having [-FIO,HDB] instance(s).....
 azureuser@fiorivm2:~ $ rm file1

 Please note that executed command : 'rm' is a restricted command ....

 you may need to have password to execute this further : [redacted] executing the restricted command now...

DONE..

[CRITICAL SYSTEM] - NEAR-PRODUCTION system having [-FIO,HDB] instance(s).....
 azureuser@fiorivm2:~ $ ls -latr file*
-rw-r----- 1 azureuser users 0 Jun 15 11:09 file2

[CRITICAL SYSTEM] - NEAR-PRODUCTION system having [-FIO,HDB] instance(s).....
 azureuser@fiorivm2:~ $
```

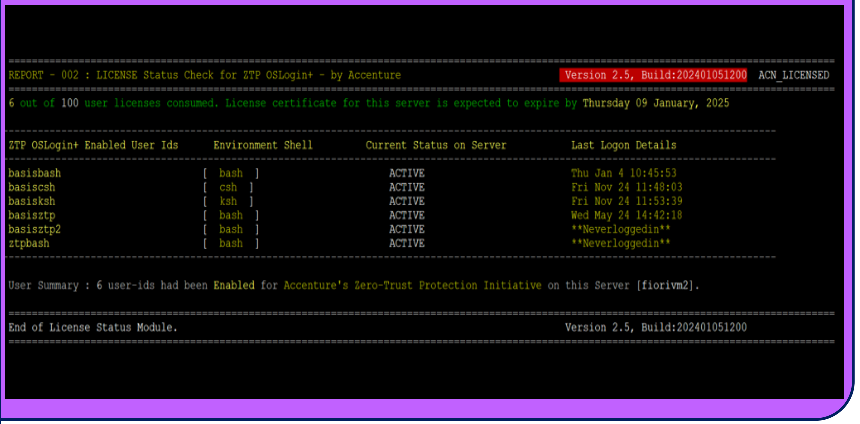
Reports at Glance

User Login Ageing Report



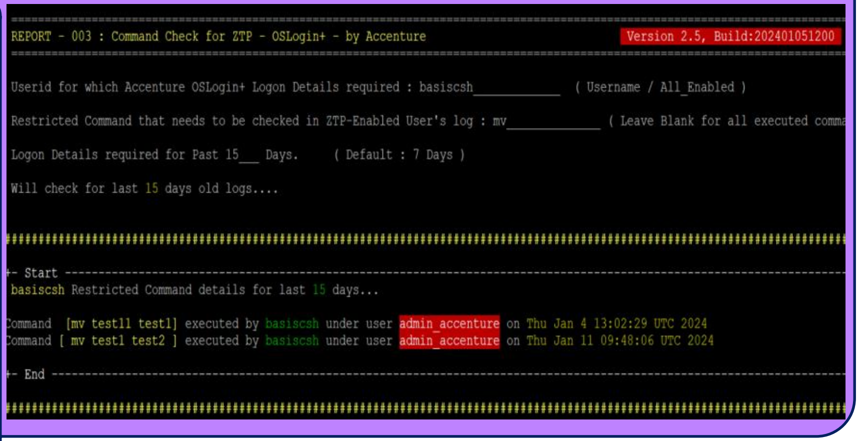
```
====================================================================================================
REPORT - 001 : ZERO TRUST PROTECTION - OSLogin+ - by Accenture              Version 2.5, Build:202308281100
====================================================================================================

====================================================================================================

Userid for which Accenture OSLogin+ Logon Details required : basisztp1__________  Username / All_Enabled

Logon Details required for Past 30___ Days.


basisztp1 Login details ...
| 1.    Terminal Session Owner, sujoym with user id admin_accenture had logged-in to the server fiorivm2
|       on Tue Aug 29 06:43:39 UTC 2023 that has SAP_APPL ==> S4H with System ID [ FIO ] installed.
--
| 1.    Terminal Session Owner, karthic.raj with user id admin_accenture had logged-in to the server fiorivm2
|       on Thu Aug 31 10:03:56 UTC 2023 that has SAP_APPL ==> S4H with System ID [ FIO ] installed.
--
| 1.    Terminal Session Owner, karthic.raj with user id basisztp1 had logged-in to the server fiorivm2
|       on Fri Sep  1 07:09:15 UTC 2023 that has SAP_APPL ==> S4H with System ID [ FIO ] installed.
--
| 1.    Terminal Session Owner, sujoy with user id admin_accenture had logged-in to the server fiorivm2
|       on Mon Sep  4 09:31:43 UTC 2023 that has SAP_APPL ==> S4H with System ID [ FIO ] installed.
--
| 1.    Terminal Session Owner, sujoym with user id admin_accenture had logged-in to the server fiorivm2
|       on Mon Sep  4 10:19:16 UTC 2023 that has SAP_APPL ==> S4H with System ID [ FIO ] installed.
--
| 1.    Terminal Session Owner, karthic.raj with user id basisztp1 had logged-in to the server fiorivm2
|       on Fri Sep  8 11:30:32 UTC 2023 that has SAP_APPL ==> S4H with System ID [ FIO ] installed.

fiorivm2:/home/azureuser/Development/acn_ztp_oslogin/ver_2.5 #
```

License Check Status Report



```
====================================================================================================
REPORT - 002 : LICENSE Status Check for ZTP OSLogin+ - by Accenture     Version 2.5, Build:202401051200  ACN_LICENSED
====================================================================================================
6 out of 100 user licenses consumed. License certificate for this server is expected to expire by Thursday 09 January, 2025

-------------------------------------------------------------------------------------------
ZTP OSLogin+ Enabled User Ids     Environment Shell      Current Status on Server     Last Logon Details
-------------------------------------------------------------------------------------------
basisbash                        [  bash  ]                 ACTIVE                  Thu Jan 4 10:45:53
basiscsh                         [  csh  ]                  ACTIVE                  Fri Nov 24 11:48:03
basisksh                         [  ksh  ]                  ACTIVE                  Fri Nov 24 11:53:39
basisztp                         [  bash  ]                 ACTIVE                  Wed May 24 14:42:18
basisztp2                        [  bash  ]                 ACTIVE                  **Neverloggedin**
ztpbash                          [  bash  ]                 ACTIVE                  **Neverloggedin**
-------------------------------------------------------------------------------------------

User Summary : 6 user-ids had been Enabled for Accenture's Zero-Trust Protection Initiative on this Server [fiorivm2].

====================================================================================================
End of License Status Module.                                           Version 2.5, Build:202401051200
====================================================================================================
```

Executed Command Check Report



```
====================================================================================================
REPORT - 003 : Command Check for ZTP - OSLogin+ - by Accenture                  Version 2.5, Build:202401051200
====================================================================================================

Userid for which Accenture OSLogin+ Logon Details required : basiscsh__________  ( Username / All_Enabled )

Restricted Command that needs to be checked in ZTP-Enabled User's log : mv__________  ( Leave Blank for all executed comma

Logon Details required for Past 15___ Days.    ( Default : 7 Days )

Will check for last 15 days old logs....


####################################################################################################

+- Start -------------------------------------------------------------------------------------------
 basiscsh Restricted Command details for last 15 days...

Command  [mv testl1 test1] executed by basiscsh under user admin_accenture on Thu Jan 4 13:02:29 UTC 2024
Command [ mv test1 test2 ] executed by basiscsh under user admin_accenture on Thu Jan 11 09:48:06 UTC 2024

+- End ---------------------------------------------------------------------------------------------

####################################################################################################
```

Copyright © 2024 | CPM – Cloud First |
Accenture Confidential | All rights Reserved

Who can Use ZTP OSLogin+

S.No.	Functionality	Who May Use	Who Can Not Use
1	ZTP OSLogin+ Version 2.5	All Linux users with local dedicated home directory can be **enabled** to use OSLogin+	Windows Based users and other NON-Linux Environment. As of now the package is compatible and tested ONLY for Linux environment (SLES,RHEL and OEL)
2	ZTP Server Login Validation & ZTP Prompt Modules	All Linux users who **enabled** to use ZTP OSLogin+ and are on bash, Ksh or sh/zsh Shell environment	Not applicable for Linux users with C-Shell* Environment.
3	Restricted Command Control Module	All Linux users who are **enabled** to use ZTP OSLogin+ (bash, ksh, csh, sh/zh)	Linux users who are NOT enabled for ZTP OSlogin+

*** Note : Linux users who has C-shell based environment and are enabled for ZTP OSLogin+ VERSION 2.5 :**

- Will be refrained from using the ZTP Server Login Validation Module, however,
- Will be enabled to use System Prompt Shell Module and Restricted Command Module with suitable pass-phrase

Caution for SAP Database User-id :

We are still trying to test the functionality for SAP Database user-ids.

HANA Database user-id <sid>adm running on sh/bash shell environment seems to have some environmental setup issue.

Please test it in non-production for your landscape, before deploying to production SAP Database users. Use ztp_uninstall program for the database user-ids, if you see issues.

Copyright © 2024 | CPM – Cloud First |
Accenture Confidential | All rights Reserved

Video Demonstration

https://mediaexchange.accenture.com/media/t/1_hs82mgcf

Copyright © 2024 | CPM – Cloud First |
Accenture Confidential | All rights Reserved

Key Contacts

For technical details, training and deployment, please contact:

Karthic Raj
karthic.raj@accenture.com

Sujoy Mukherjee
sujoy.s.mukherjee@accenture.com

Dibya Ranjan Das
dibya.ranjan.das@accenture.com

Prashant S Patil
prashant.patil@accenture.com

SPONSORS

Mukesh Chaudhary
Cloud First Director of Delivery
mukesh.chaudhary@accenture.com

Ketan N. Shah
ketan.n.shah@accenture.com

Sanjeev Ahuja
sanjeev.ahuja@accenture.com

Copyright © 2024 | CPM – Cloud First | Accenture
Confidential | All rights Reserved

THANK YOU