

דוגמה לטיפול באסקלציה

הודעה מהתחמיכה

Hi AIM R&D,

My customer has opened a case with us in regards to their Linux providers

Unix servers

- CP v14.00
- CLIPasswordsdk

After a recent OS Patch which I'm still trying to have the customer confirm which one. The customers Linux Providers have started to fail Allowed Machine Authentication. The Providers were whitelisted in the Application's authentication list with their short hostname name.

After the patch the customer is needing to add the IP/ FQDN under allowed machines of Application created in CyberArk. The issue here is that the customer has 100's of applications.

The has found that the patch removed an entry from the host file.

Customer would like to confirm if aimagent is depending on etc\hostfile for shortname? If not, what could be the reason for sudden break in the configuration.

```
[sysabc @SGDPSR00002][PROD]: sysabc > hostname -f  
SGDP.int.bar.com  
[sysabc @ SGDPSR00002][PROD]: sysabc > hostname -s  
SGDPSR00002
```

I have found the following Article <https://community.cyberark.com/s/article/How-does-the-Application-Password-Provider-determine-server-s-IP-address> however speaking with Diego, there was mention of an API call.

If we can confirm how we obtain the and attach the hostname to the call, I think this would greatly help Barclays with a plan on how they can reverse/amend the settings which has triggered the change in behaviour for them rather than mass updates to the Application information.

Please do let me know if there is further information you would like to see.

Best regards,
Manuel Ortega

תשובה ללקוח על ידי הפיתוח

Hi Daniel

The FQDN apparently changed from the Linux upgrade

In Linux, the FQDN is determined from the "hostname -f" command.

What Diego talks about with the api call is relevant for Windows.

CP blocks every communication and password request from unknown hostname, hence if host name was changed it will block all of the requests (from this unauthorized end point)

The client should update his application's authentication list with the new hostnames

ניתוח תשובה ללקוח על ידי הפיתוח

1 - טון התשובה

בעיה: הטון חד מדי ונשמע מאשים.

לדוגמה: "...CP blocks every communication
המשפט מציג את הבעיה קטעות של הלקוח, במקומ להראות שאנו בצוות פועלים יחד.

шиפור:

להשתמש בטון שיתופי ומלואה, שמראה שאנו חלק מהפתרון.
"I understand the situation, and we are here to help..."

2 - הבנת הבעיה

בעיה: חסר הסבר ברור על מה הבנו מהבעיה ומה היא השפעתה.
הלקוח צריך לראות שאנו מבינים את הסיבה לבעה, לא רק תוצאה טכנית.

шиפור:

להויסיף משפט פתיחה שמסכם את מה שהלקוח חווה והבנתנו את השורש:
"I understand that the application stopped receiving passwords after the Linux upgrade, and the FQDN change caused the CP to treat the server as an unrecognized source."

3 - מה אנחנו עושים עכשווי

בעיה: חסר הסבר ברור על הצעדים שאנו נוקטים כרגע.

шиפור:

לפרט את הפעולות שלנו בצורה מלאה וברורה:
"We will validate the logs they sent and reproduce the scenario in-house to suggest the proper fix."
"I will guide them step by step if anything is unclear."

ביתוח תשובה ללקוח על ידי הפיתוח

4 - מבנה כללי

בעיה: אין מבנה ברור – קורה, משמעות, מה עושים.

שיפור:

לארגן את התשובה לפי שלושה חלקים:

מה קרה: שינוי ה-FQDN אחרי השדרוג.

מה המשמעות: CP חוסם את כל הבקשות מהשרת כי הוא לא מזוהה.

מה עושים: צעדים מיידיים (עדכון רשימת אימוט, בדיקה מחדש, ליווי הלקוח).

5 - אחריות ופעולות לckoח

בעיה: המשפט האחרון מגלה אחריות ללקוח בלי ללבות אותו.

לדוגמה: "The client should update..." נשמע שהלקוח לבד.

שיפור:

להוסיף ליווי והכוונה:

"We can guide them through updating the authentication list and confirming the configuration."

6 - בהירות בין מערכות הפעלה

בעיה: ערבות בין Linu^x ל-Windows בלי הסבר למה זה רלוונטי.

שיפור:

להבהיר את ההבדלים והקשר:

"The FQDN change is specific to Linux. The API call Diego mentioned is relevant for Windows environments, so this detail does not apply here."

סיכון נקודות לשיפור בתשובה ל Koh Mackzouyah

- טון שיתופי, לא מאשים.
- הסבר ברור על מה שהבנו מהבעיה.
- פירוט פעולות שאנו מבצעים עכשו.
- מבנה מסודר: מה קרה ← מה המשמעות ← מה עושים.
- ליווי הלקוח בכל שלב, לא להעביר אחריות בלבד.
- הבהרה בין מערכות הפעלה רלוונטיות.

תשובה סופית ללקוחה

Hi Daniel,

I understand that the customer reports the application stopped receiving passwords from the CP after the Linux upgrade. Based on the behavior and the logs they shared, the CP now treats the server as an unrecognized source.

The upgrade introduced a new FQDN.

The hostname -f output shows a different value, and this change affects how the CP matches the server in the authentication list. When the hostname changes, the CP identifies the server as an unauthorized endpoint and blocks every request.

Next steps

- We will review the logs they send so we can confirm the behavior
- I will reproduce the scenario in-house to analyze it and suggest the correct fix
- I will guide you through each step if anything is unclear

I'll update you within 24 hours with initial findings.

In the meantime, if the customer cannot proceed until we present a full solution, please ask them to:

- Add the new hostname to the authentication list
- Confirm that the updated FQDN appears in the configuration
- Restart the relevant service after the update

**Internal note to support

Please guide the customer in each step on what they need to do

Thank you for your collaboration.

Please let me know if you require any additional clarification.

Best regards,
[Your Name]