Got it — I’ll break this down clearly in simple terms so you can understand what’s going on in that discussion.

### **Context:**

* The team is using **BeyondTrust** (likely for privileged access management and system scanning).
* Most systems are hosted on **AWS EC2 instances**, with a few on-prem servers.
* When BeyondTrust scans systems, it tries to get both the **IP address** and the **DNS name** of each system.
* The **DNS name** should be something meaningful (e.g., server1.company.com) so people can identify the system easily.

### **Problem:**

1. **DNS Name is not user-friendly:**
   * Many AWS systems are coming in with names like ip-172-31-xx-xx.ec2.internal.
   * This is an internal AWS DNS name, not a user-friendly one.
   * As a result:  
     + **RDP (Remote Desktop)** connections work because IPs are correct.
     + But BeyondTrust can’t show a meaningful system name, so admins/users can’t easily identify what system it is.
2. **Impact:**
   * Some systems show only a **single shield symbol** in BeyondTrust → means they were **scanned** but **not managed** properly.
   * For systems with meaningful DNS names, BeyondTrust can manage them correctly.
   * For systems with EC2 internal names, BeyondTrust can’t properly manage them.

### **Possible Causes:**

* AWS EC2 by default assigns **internal hostnames** like ec2.internal.
* If reverse DNS lookup (nslookup) doesn’t return the correct custom DNS name, BeyondTrust just gets the internal AWS name.
* This could be because:  
  + Proper DNS records (PTR or A records) are not configured in your organization’s DNS server.
  + AWS hostnames are not mapped to friendly names in Route 53 or internal DNS.

### **Suggested Next Steps from the Discussion:**

1. **Open a support ticket** with BeyondTrust:  
   * Give them examples of affected systems.
   * Ask why these systems are not getting proper names during scans.
2. **If needed, schedule a call** with BeyondTrust support:  
   * Between 8–10 AM IST so that the senior person can join for any additional queries.
3. **Troubleshooting approach:**
   * Start fresh because previous attempts (in 2023) didn’t lead to a fix since it wasn’t a priority then.
   * Check DNS configurations:  
     + Does reverse DNS mapping exist for these systems?
     + Are custom DNS names assigned in AWS or internal DNS?
   * Confirm if BeyondTrust needs DNS changes or tool-side configurations.

### **Key Takeaways:**

* **IPs are correct, but DNS names are wrong**, so BeyondTrust can’t display user-friendly names.
* Root cause is likely **DNS reverse lookup or naming standards** in AWS.
* Fix involves **working with BeyondTrust** and possibly **network/DNS teams** to ensure systems have meaningful DNS names.

If you want, I can create a **step-by-step troubleshooting checklist** for this issue so you can approach it methodically.

Do you want me to prepare that?

##### **You said:**

what should be there in support ticket, give very tecgnical description toinclude in the ticket?

###### **ChatGPT said:**

Got it. For the support ticket to BeyondTrust, you want to give a **clear, technical description** with **evidence, environment details, and expected outcome** so that they can reproduce and assist effectively.

Here’s what you should include in the ticket:

### **Subject**

BeyondTrust: Systems Resolving with EC2 Internal Hostnames Instead of User-Friendly DNS Names

### **Description for the Ticket**

**Issue Summary:** We are facing an issue where certain AWS-hosted systems appear in BeyondTrust scans with DNS names in the format ip-xx-xx-xx-xx.ec2.internal instead of the expected user-friendly DNS names (e.g., hostname.domain.com). This prevents BeyondTrust from correctly identifying and managing these systems.

**Environment Details:**

* **BeyondTrust Product:** [e.g., BeyondTrust Password Safe / BeyondInsight]
* **Version:** [Version details]
* **OS of affected systems:** AWS EC2 Windows/Linux instances
* **Percentage of systems affected:** ~90% AWS-hosted systems
* **On-prem systems:** Mostly unaffected; issue seen primarily on AWS

**Observed Behavior:**

* Systems discovered via BeyondTrust scans show correct **IP addresses** but the **DNS Name** field resolves to \*.ec2.internal.
* These systems display only the **single shield** icon in BeyondTrust → indicating they are **scanned but not managed**.
* Performing an nslookup or reverse DNS lookup on the IP address from BeyondTrust returns only the AWS internal DNS name (ec2.internal) instead of the expected custom DNS name.
* Example of affected system:  
  + **IP:** 172.31.xx.xx
  + **DNS Name returned:** ip-172-31-xx-xx.ec2.internal
  + **Expected DNS Name:** appserver01.its.domain.com

**Impact:**

* Users cannot easily identify systems in BeyondTrust UI for RDP or privileged access.
* BeyondTrust cannot manage affected systems due to missing friendly DNS names.
* Limits visibility and automation for password management and session handling.

**Steps Already Tried / History:**

* Checked DNS configuration; on-prem systems resolve correctly.
* AWS instances do not appear to have reverse DNS entries mapping IP → user-friendly DNS name.
* This issue was partially investigated in 2023 but deprioritized due to other priorities; no permanent fix yet.

**Expectation:**

* BeyondTrust should either:  
  1. Resolve AWS instances to their correct user-friendly DNS names (e.g., via reverse lookup).
  2. Provide configuration/workaround if AWS internal DNS naming conflicts with BeyondTrust discovery.
  3. Suggest best practices for DNS integration with AWS-hosted systems for accurate BeyondTrust scans.

**Attachments (Recommended):**

1. Screenshots from BeyondTrust UI showing affected systems.
2. nslookup command output from BeyondTrust scanning server for affected IPs.
3. CSV or list of sample affected IPs and their current vs. expected DNS names.

**Additional Info:**

* Please advise if BeyondTrust relies solely on reverse DNS lookups or if there is an option to map IPs to friendly names via alternate configuration.
* If additional logs or debug traces are needed, we can provide them.

If you want, I can draft a **ready-to-copy technical ticket** for you with all placeholders filled in so you can directly raise it in the BeyondTrust support portal.

Do you want me to prepare that?