# Entra Cloud Sync / gMSA Troubleshooting Guide

How we fixed the Entra Provisioning Agent error on **HQ-DC01** when Active Directory could not resolve the **Managed Service Accounts** container correctly.

**Summary:** The final root cause was not just permissions or the existence of the `CN=Managed Service Accounts` container. The real issue was that the domain's `otherWellKnownObjects` attribute still pointed the Managed Service Accounts GUID to a **deleted object** under `CN=Deleted Objects`. Removing the stale `\0ADEL` reference and restoring the live mapping fixed the problem.

## 1. Environment

- **Domain:** aspirapa.org
- **Server used for repair:** HQ-DC01
- **Issue surface:** Entra Provisioning Agent / Entra Cloud Sync setup
- **Symptom:** The wizard failed while trying to create or locate the Managed Service Account container

## 2. Original Symptoms

During the Entra Cloud Sync setup, the wizard reported that it could not find the **Managed Service Accounts** container. Earlier troubleshooting also uncovered several foundational Active Directory issues that had to be corrected before the final fix would succeed.

> **Important:** This repair was the final step in a larger cleanup. Earlier problems included an outdated domain functional level, stale domain controller metadata, and DNS / domain discovery problems. Those needed to be addressed first.

## 3. Earlier Problems That Were Addressed First

Before the final container mapping repair, the following issues were identified and worked through:

1. **Domain functional level was too old.**
   The domain was initially identified as `Windows2008Domain`. This was raised to **Windows Server 2012 R2 domain functional level**, which is necessary for modern gMSA and Entra-related workflows.
2. **Old DC metadata needed cleanup.**
   Legacy domain controllers such as `CYBERDC01` and `ASPIRADC1` were no longer present and required metadata cleanup, including NTDSUTIL cleanup, DNS cleanup, and review of Active Directory Sites and Services.
3. **KDS root key and gMSA prerequisites were reviewed.**
   KDS keys were checked and a new KDS root key was added as part of the process.
4. **DNS / secure channel discovery was broken.**
   `nltest /sc_verify` failed with `1355 ERROR_NO_SUCH_DOMAIN`. The NIC DNS configuration was corrected so the domain controller pointed to internal AD DNS only, and DNS / SRV discovery tests were rerun successfully.
5. **Managed Service Accounts container checks were performed.**
   Eventually, `CN=Managed Service Accounts,DC=aspirapa,DC=org` was confirmed to exist, which proved that the final error was not simply “missing container.”

## 4. What Did Not Work

- Attempting to treat the issue as only a permissions problem
- Assuming the error meant the container did not exist
- Trying to add the mapping to `wellKnownObjects` instead of the correct attribute
- Trying to force the repair through LDP while the wrong target attribute was being used

> **Key lesson:** In this case, the Managed Service Accounts GUID was already present in the directory metadata, but it pointed to a deleted object. That is why the live container existed while the Entra agent still failed.

# 5. How the Real Root Cause Was Found

PowerShell inspection of the domain root object showed that the built-in `wellKnownObjects` attribute did not contain the MSA mapping, but the `otherWellKnownObjects` attribute did. The problem was that the MSA GUID `1EB93889E40C45DF9F0C64D23BBB6237` pointed to a deleted object path instead of the live container.

## Command used to inspect the live domain root mapping

```
Get-ADObject "DC=aspirapa,DC=org" -Properties otherWellKnownObjects |
Select-Object -ExpandProperty otherWellKnownObjects
```

## Problematic output

```
B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=aspirapa,DC=org
B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service
Accounts\0ADEL:5b87c493-325b-45b2-9c8c-bd17424d981b,CN=Deleted
Objects,DC=aspirapa,DC=org
```

That second line was the smoking gun. The MSA GUID existed, but it referenced a deleted object instead of:

```
CN=Managed Service Accounts,DC=aspirapa,DC=org
```

# 6. Final Repair That Worked

The successful repair was to remove the stale deleted-object mapping from `otherWellKnownObjects` and replace it with the correct live container mapping.

## PowerShell repair commands

```
$dn = "DC=aspirapa,DC=org"

$bad = "B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service
Accounts\0ADEL:5b87c493-325b-45b2-9c8c-bd17424d981b,CN=Deleted
Objects,DC=aspirapa,DC=org"
$good = "B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service
Accounts,DC=aspirapa,DC=org"

Set-ADObject -Identity $dn -Remove @{otherWellKnownObjects=$bad}
Set-ADObject -Identity $dn -Add @{otherWellKnownObjects=$good}

Get-ADObject $dn -Properties otherWellKnownObjects |
Select-Object -ExpandProperty otherWellKnownObjects
```

### Expected good result

```
B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service
Accounts,DC=aspirapa,DC=org
```

### Replication after repair

```
repadmin /syncall /AdeP
```

## 7. Verification Steps

1. Confirm the stale `\0ADEL` reference is gone from `otherWellKnownObjects`.
2. Confirm the live mapping exists for the MSA GUID.
3. Run replication.
4. Return to the Entra Provisioning Agent wizard and click **Confirm** again.
5. Verify that the agent now proceeds without the Managed Service Accounts container error.

### Useful verification commands

```
Get-ADObject "CN=Managed Service Accounts,DC=aspirapa,DC=org"

Get-ADObject "DC=aspirapa,DC=org" -Properties otherWellKnownObjects |
Select-Object -ExpandProperty otherWellKnownObjects

repadmin /syncall /AdeP
```

## 8. Full Recommended Troubleshooting Flow for Similar Cases

1. **Check domain functional level** and raise to at least 2012 / 2012 R2 if required.
2. **Clean stale DC metadata** for removed domain controllers.
3. **Check DNS client settings** on domain controllers and ensure they point only to internal AD DNS servers.
4. **Validate domain discovery** with `nltest`, `dcdiag`, and DNS SRV lookups.
5. **Confirm KDS root key** and other gMSA prerequisites.
6. **Confirm the live MSA container exists**.
7. **Inspect both** `wellKnownObjects` **and** `otherWellKnownObjects`.
8. **If the MSA GUID points to a deleted object, repair the mapping**.
9. **Sync replication** and rerun the Entra provisioning workflow.

## 9. Why This Matters

This issue can mislead administrators because the `Managed Service Accounts` container may exist and still not be resolvable by Entra or gMSA-related tools. The issue is not always the container itself. It can be the **directory reference to that container**.

> **Final outcome:** After removing the stale deleted-object entry and adding the correct live `otherWellKnownObjects` mapping, the Entra Cloud Sync / Provisioning Agent error was resolved successfully.

# 10. Copy/Paste Quick Reference

```
# Inspect the current mapping
Get-ADObject "DC=aspirapa,DC=org" -Properties otherWellKnownObjects |
Select-Object -ExpandProperty otherWellKnownObjects

# Repair the stale deleted-object reference
$dn = "DC=aspirapa,DC=org"
$bad = "B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service
Accounts\0ADEL:5b87c493-325b-45b2-9c8c-bd17424d981b,CN=Deleted
Objects,DC=aspirapa,DC=org"
$good = "B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service
Accounts,DC=aspirapa,DC=org"

Set-ADObject -Identity $dn -Remove @{otherWellKnownObjects=$bad}
Set-ADObject -Identity $dn -Add @{otherWellKnownObjects=$good}

# Verify the fix
Get-ADObject $dn -Properties otherWellKnownObjects |
Select-Object -ExpandProperty otherWellKnownObjects

# Replicate
repadmin /syncall /AdeP
```

---

Prepared for BookStack HTML use. This page is designed to be pasted into a BookStack HTML editor or imported as a standalone HTML reference.

---

Revision #4
Created 2026-04-07 04:30:02 UTC by joliveira
Updated 2026-04-07 14:33:28 UTC by joliveira