Troubleshoot Umbrella Errors for Active Directory and VAs

Contents

Introduction

Issue

Environment

Resolution

- Virtual Appliances
  - "This VA has registered but has never synced"
  - "This VA was syncing at one point but has since stopped"
  - "This VA was previously connected to one or more Connectors, but is now connected to none"
  - "This Virtual Appliance is connected to some, but not all, of the Connectors for this site"
  - "DNS queries forwarded by this VA to Umbrella are not encrypted"
  - "This VA does not have any local domains configured"
  - "This VA is not redundant within its site (2+ VA required per site)"
  - "A large percentage of DNS queries to this VA are failing"
- AD Connectors
  - "This Connector has registered but has never synced"
  - "This Connector was syncing at one point but has since stopped"
  - "This Connector has either no VA or no DC to connect to"
  - "This Connector has no DC to connect to"
  - "There are one or more DCs that the Connector could connect to, but it has not connected to any yet"
  - "The Connector is connected to some, but not all, DCs"
  - "The Connector was once connected, but is not currently connected to any of the DCs available"
  - "There are one or more VAs that the Connector could connect to, but it has not connected to any yet"
  - "The Connector is reporting timeout errors while attempting to connect to some VAs"
  - "The Connector is connected to some, but not all, VAs"
  - "The Connector was once connected but is not currently connected to any of the VAs available"
  - "The Connector is not syncing events in parallel to VAs. Events processing can be slower than expected"
  - "The Connector is reporting drops while attempting to send events to some VAs"
- Domain Controllers
  - "Was at one point connected to one or more Connectors but is now connected to none"
  - "This Domain Controller has never connected to a Connector"
  - "This Domain Controller has no Connectors to connect to"
  - "This Domain Controller is connected to some, but not all, Connectors"
  - "WMI state of this Domain Controller is down. The Domain Controller is not responding to the WMI connection from the Connector"

Causes

Related Content

Introduction

This document describes troubleshooting Umbrella errors for Active Directory and Virtual Appliances.

Issue

This document outlines common error, warning, and informational messages on the Sites and Active Directory page and provides resolution steps.

One or more error, warning, or informational messages appear on the Umbrella **Settings** > **Sites and AD** page for Virtual Appliances, Active Directory (AD) Connectors, or Domain Controllers (DCs).

Environment

The Umbrella Sites and Active Directory page is located at **Settings** > **Sites and AD**.

- Affected components include Virtual Appliances (VAs), AD Connectors, and DCs.
- DNSCrypt support is available in VA version 1.5.x or later.
- If the connector is deployed on Windows Server (WS) 2012 or greater and stopped syncing to Umbrella, ensure that the connector is running version 1.6.31 or higher.
- Connectors version 1.6.31 or higher function on WS 2008/2008 R2 if running .NET 4.5.2 or higher, but redeployment on a supported server is recommended.
- Cisco announced End of Life (EOL) of Transport Layer Security (TLS) 1.0/1.1. Unsupported Windows versions (Windows Server 2008, 2008 R2, or Windows 7) do not support TLS 1.2 by default. Reinstall the connector on a supported server version (Windows Server 2012 or higher).
- To send login event information to a Virtual Appliance, the Domain Controller (DC) must have a Connector installed in the same site.
- Sites must contain at least one of each component type where noted by the message.
- The Umbrella Connector service is tested to support 10 assets (Domain Controllers and Virtual Appliances) per CPU.
- The Umbrella Connector service is tested to support approximately 850 continuous events (no hard limit) per second across all Domain Controllers in an Umbrella Site.

Resolution

Use the section that matches the component type shown on **Settings** > **Sites and AD**, then select the exact message text.

- **Virtual Appliances**: VA registration/sync status, Connector association, DNSCrypt, local domains, redundancy, and DNS query failure messages.
- **AD Connectors**: Connector registration/sync status, DC/VA connectivity, timeouts, parallel processing, and event drop messages.
- **Domain Controllers**: Connector association and WMI connectivity messages.

Virtual Appliances

"This VA has registered but has never synced"

1. Allow up to 10 minutes for syncing to complete.
2. Ensure the network requirements are met. See Guide to Active Directory Communication Flow: **Connectors** > **Virtual Appliances** > **DCs and the Cloud**.
3. If the issue persists, collect logs and open a support case.

"This VA was syncing at one point but has since stopped"

Use these steps to restore VA synchronization and confirm required connectivity.

1. If the VA was deleted, remove it from the Umbrella dashboard: Removal Instructions - Umbrella Insights.
2. Confirm the network requirements. See Guide to Active Directory Communication Flow: **Connectors** > **Virtual Appliances** > **DCs and the Cloud**.
3. Open a support case if the problem persists.

"This VA was previously connected to one or more Connectors, but is now connected to none"

1. If any Connectors were removed, ignore this message and remove the stale Connector entry from the dashboard.
2. Confirm the network requirements. See Guide to Active Directory Communication Flow: **Connectors** > **Virtual Appliances** > **DCs and the Cloud**.
3. Open a support case if the problem persists.

"This Virtual Appliance is connected to some, but not all, of the Connectors for this site"

1. If any Connectors were removed, ignore this message and remove the Connector from the dashboard.
2. Confirm prerequisites: Virtual Appliance User Guide: Prerequisites.
3. Collect logs: Providing support with AD connector logs.
4. Open a support case if the problem persists.

"DNS queries forwarded by this VA to Umbrella are not encrypted"

DNSCrypt encrypts DNS packets forwarded from the Virtual Appliance (VA) to Umbrella public DNS resolvers and is enabled by default.

1. Confirm the VA is running version 1.5.x or later. DNSCrypt support is available in 1.5.x or later. If only one VA exists and it is not upgraded, upgrade it: Update Virtual Appliances.
2. Review firewall and inspection policies to ensure the DNSCrypt probe on port 53 (UDP/TCP) is not blocked or altered. If an Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) performs deep packet inspection and expects only DNS traffic, the probe can fail.
3. For Adaptive Security Appliance (ASA) deployments, review the packet inspection guidance

referenced by the deployment documentation.
4. If the warning persists, collect logs: Providing support with AD connector logs, then open a support case.
5. Verify the warning clears on **Settings** > **Sites and AD** for the affected VA.

More details: New VA Warning: Enabling DNSCrypt on your Virtual Appliance.

"This VA does not have any local domains configured"

1. Ensure local domains are configured: Local DNS Forwarding.

"This VA is not redundant within its site (2+ VA required per site)"

1. Install a second VA for high availability. Refer to your Umbrella Virtual Appliance deployment documentation for guidance on running two Virtual Appliances per site.

"A large percentage of DNS queries to this VA are failing"

1. Collect relevant VA and Connector logs and open a support case.
2. Verify the DNS query failure rate returns to normal and the error clears on **Settings** > **Sites and AD** for the affected VA.

AD Connectors

"This Connector has registered but has never synced"

Use these checks to confirm initial synchronization completes successfully:

1. Allow up to 10 minutes for syncing to complete.
2. Ensure the network requirements are met: Identity Integrations: Prerequisites.
3. Collect logs: Providing support with AD connector logs.
4. Open a support case if the problem persists.

"This Connector was syncing at one point but has since stopped"

1. Ensure the network requirements are met. See Guide to Active Directory Communication Flow: **Connectors** > **Virtual Appliances** > **DCs and the Cloud**.
2. Cisco announced EOL of TLS 1.0/1.1. Unsupported Windows versions (Windows Server 2008, 2008 R2, or Windows 7) do not support TLS 1.2 by default. Reinstall the connector on a supported server version (Windows Server 2012 or higher).
3. If the connector is deployed on WS 2012 or greater and stopped syncing to Umbrella, ensure that the

connector is running version 1.6.31 or higher.
4. Connectors version 1.6.31 or higher function on WS 2008/2008 R2 if running .NET 4.5.2 or higher, but redeployment on a supported server is recommended.
5. Collect logs: Providing support with AD connector logs.
6. Open a support case if the problem persists.

"This Connector has either no VA or no DC to connect to"

1. Ensure the site contains at least one of each component type.
2. Review setup documentation: Identity Integrations: Prerequisites and Active Directory Integration > **Step 2: Prepare your Active Directory Environment.**

"This Connector has no DC to connect to"

1. Ensure the site contains at least one of each component type.
2. Review setup documentation: Prepare Your Active Directory Environment.

"There are one or more DCs that the Connector could connect to, but it has not connected to any yet"

1. Allow up to 10 minutes for syncing to complete.
2. Ensure the prerequisites are met: Identity Integrations: Prerequisites.
3. Collect logs: Providing support with AD connector logs.
4. Open a support case if the problem persists.

"The Connector is connected to some, but not all, DCs"

1. Confirm prerequisites: Identity Integrations: Prerequisites.
2. Collect logs: Providing support with AD connector logs.
3. Open a support case if the problem persists.

"The Connector was once connected, but is not currently connected to any of the DCs available"

1. Confirm prerequisites: Identity Integrations: Prerequisites.
2. Collect logs: Providing support with AD connector logs.
3. Open a support case if the problem persists.

"There are one or more VAs that the Connector could connect to, but it has not connected to any yet"

1. Remove any unused VAs from the dashboard.
2. Allow up to 10 minutes for syncing after removal.
3. Ensure the network requirements are met: Identity Integrations: Prerequisites.

4. Collect logs: Providing support with AD connector logs.
5. Open a support case if the problem persists.

"The Connector is reporting timeout errors while attempting to connect to some VAs"

1. If the Virtual Appliance is not on the same LAN as the Connector, consider segregating deployment using Umbrella sites: Connect Multiple Active Directory Domains to Umbrella.
2. Remove unused VAs from the dashboard.
3. Allow up to 10 minutes for syncing after removal.
4. Ensure the network requirements are met: Identity Integrations: Prerequisites.
5. Collect logs: Providing support with AD connector logs.
6. Open a support case if the problem persists.

"The Connector is connected to some, but not all, VAs"

1. Remove unused VAs from the dashboard.
2. Allow up to 10 minutes for syncing after removal.
3. Ensure the network requirements are met. See Guide to Active Directory Communication Flow: **Connectors** > **Virtual Appliances** > **DCs and the Cloud**.
4. Collect logs: Providing support with AD connector logs.
5. Open a support case if the problem persists.

"The Connector was once connected but is not currently connected to any of the VAs available"

1. Remove unused VAs from the dashboard.
2. Allow up to 10 minutes for syncing after removal.
3. Ensure the network requirements are met: Guide to Active Directory Communication Flow: Connectors > **Virtual Appliances** > **DCs and the Cloud.**
4. Collect logs: Providing support with AD connector logs.
5. Open a support case if the problem persists.

"The Connector is not syncing events in parallel to VAs. Events processing can be slower than expected"

1. Note that the Umbrella Connector service is tested to support 10 assets (Domain Controllers and Virtual Appliances) per CPU.
2. Upgrade the server with the required number of CPUs based on the number of Domain Controllers and Virtual Appliances in the Umbrella Site.
3. Collect logs: Providing support with AD connector logs.
4. Open a support case if the problem persists.

"The Connector is reporting drops while attempting to send events to some VAs"

Use these steps to reduce event drops and restore stable event delivery.

1. Check whether the total event rate across all Domain Controllers in the Umbrella Site exceeds the tested continuous capacity of approximately 850 events per second.
2. If the event rate exceeds this tested capacity, increase CPU cores on the Connector host to improve processing throughput.
3. If drops persist, enable load-balancing with two or more Connectors to share Domain Controller load. This advanced feature must be enabled by opening a support case with Umbrella support.

Domain Controllers

"Was at one point connected to one or more Connectors but is now connected to none"

1. If the Connector was removed, either redeploy the Connector or remove the Domain Controller.
2. Confirm the network requirements. See Guide to Active Directory Communication Flow: **Connectors** > **Virtual Appliances** > **DCs and the Cloud**.
3. Collect logs: Providing support with AD connector logs.
4. Open a support case if the problem persists.

"This Domain Controller has never connected to a Connector"

1. To send information about logon events to a Virtual Appliance, the Domain Controller (DC) must have a Connector installed in the same site. See Connect Active Directory to Umbrella.
2. Collect logs: Providing support with AD connector logs.
3. Open a support case if the problem persists.

"This Domain Controller has no Connectors to connect to"

1. To send information about logon events to a Virtual Appliance, the Domain Controller (DC) must have a Connector installed in the same site. See Connect Active Directory to Umbrella.
2. If reinstalling the Connector or moving it from one machine to another, ignore this message.

"This Domain Controller is connected to some, but not all, Connectors"

1. Check permissions: Required Permissions for the Cisco_Connector User.
2. Collect logs: Providing support with AD connector logs.
3. Open a support case if the problem persists.

"WMI state of this Domain Controller is down. The Domain Controller is not responding to the WMI connection from the Connector"

1. This can be a temporary problem due to the load on the Domain Controller.
2. Check if the Windows Management Instrumentation (WMI) connection can be established using the WBEMTest tool.
3. Reduce the load on the DC by stopping other unused applications monitoring security events.
4. Restart the Connector service to initiate a fresh WMI connection after reducing DC load.
5. Collect logs: Providing support with AD connector logs.
6. Open a support case if the problem persists.

Causes

- **DNSCrypt warning messages (VA)**: DNSCrypt is enabled by default to encrypt DNS packets forwarded from the Virtual Appliance (VA) to Umbrella public DNS resolvers. If firewall or inspection policies block or alter the DNSCrypt probe on port 53 (UDP/TCP), the probe fails. If an Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) performs deep packet inspection and expects only DNS traffic, the probe fails.
- **Connector sync-stopped messages (AD Connector)**: Cisco announced End of Life (EOL) of Transport Layer Security (TLS) 1.0/1.1. Unsupported Windows versions (Windows Server 2008, 2008 R2, or Windows 7) do not support TLS 1.2 by default, which causes connector syncing to stop.
- **Connector performance messages (AD Connector)**: The Umbrella Connector service is tested to support 10 assets (Domain Controllers and Virtual Appliances) per CPU. When this sizing is exceeded, events processing is slower than expected.
- **Event drop warning messages (AD Connector)**: The Umbrella Connector service is tested to support approximately 850 continuous events (no hard limit) per second across all Domain Controllers in an Umbrella Site. If the overall rate exceeds this tested capacity, the Connector drops events.
- **WMI-down error messages (Domain Controller)**: WMI state is down when the Domain Controller is under load and does not respond to the WMI connection from the Connector.

Related Content

- Examine the Umbrella Active Directory Integration Flow
- Submit Active Directory Connector Logs to Umbrella Support