

Table of Contents

<u>Cisco CallManager: Detecting and Solving SQLSvc Password Problems</u>	1
<u>Document ID: 27540</u>	1
<u>Introduction</u>	1
<u>Prerequisites</u>	1
<u>Requirements</u>	1
<u>Components Used</u>	1
<u>Conventions</u>	1
<u>Problem 1</u>	1
<u>Solution 1</u>	4
<u>Problem 2</u>	7
<u>Solution 2</u>	8
<u>Related Information</u>	10

Cisco CallManager: Detecting and Solving SQLSvc Password Problems

Document ID: 27540

Introduction

Prerequisites

Requirements

Components Used

Conventions

Problem 1

Solution 1

Problem 2

Solution 2

Related Information

Introduction

This document enables Cisco CallManager users to detect and correct SQLSvc password–related problems.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software versions:

- Cisco CallManager 3.0, 3.1, and 3.2
- Use the AdminUtility to change the password for Cisco CallManager 3.3 and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

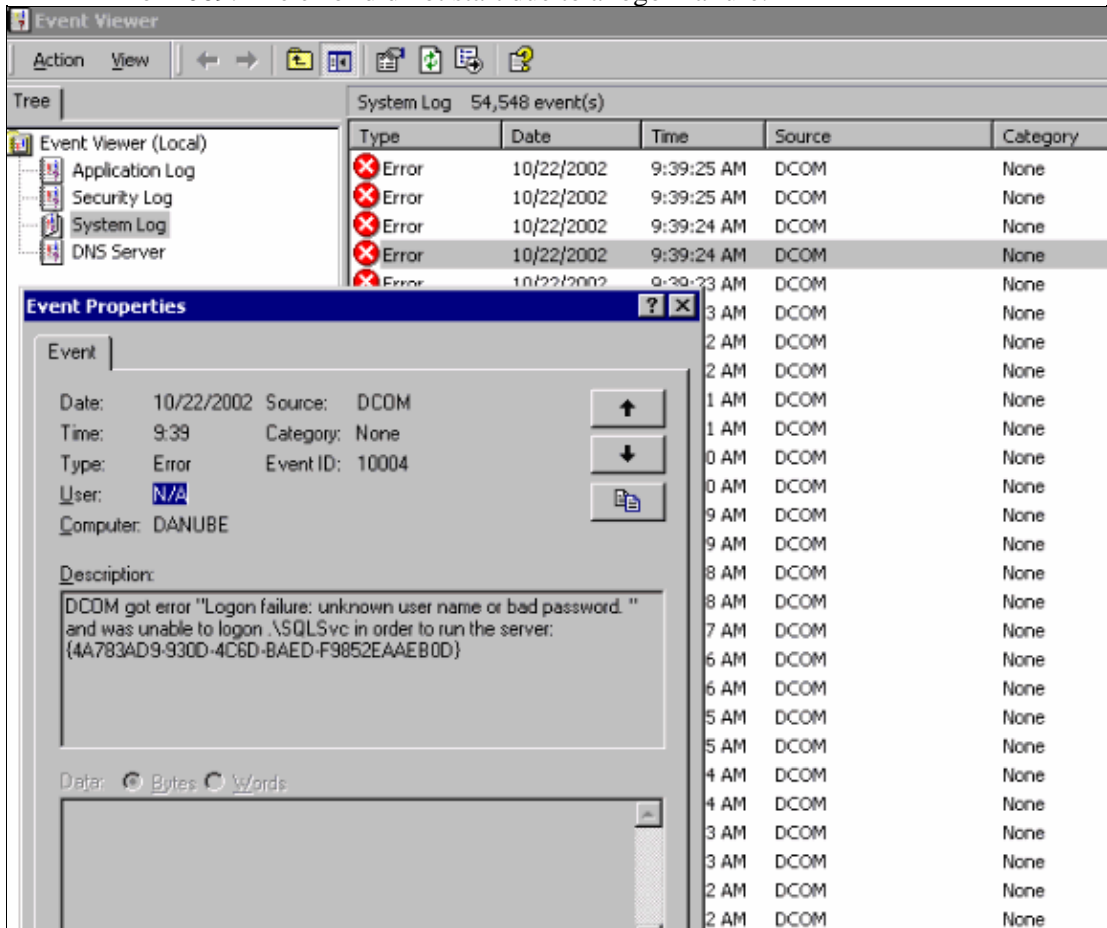
Problem 1

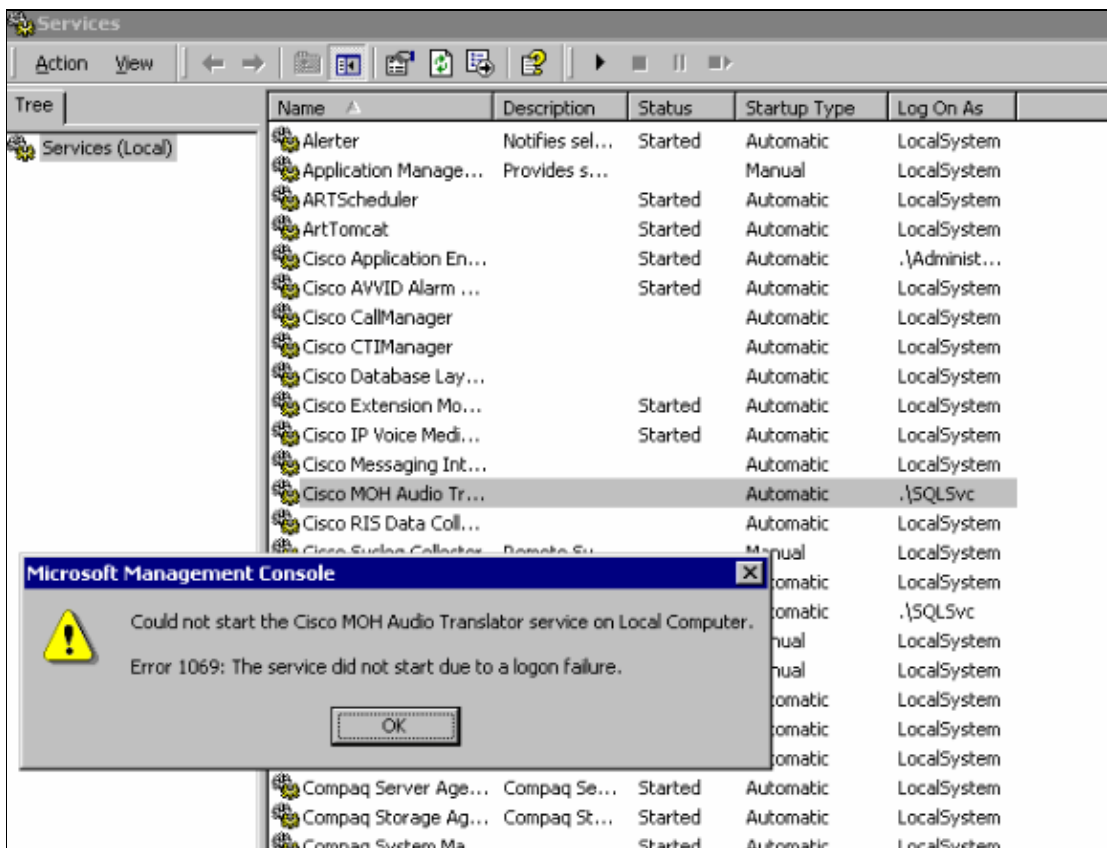
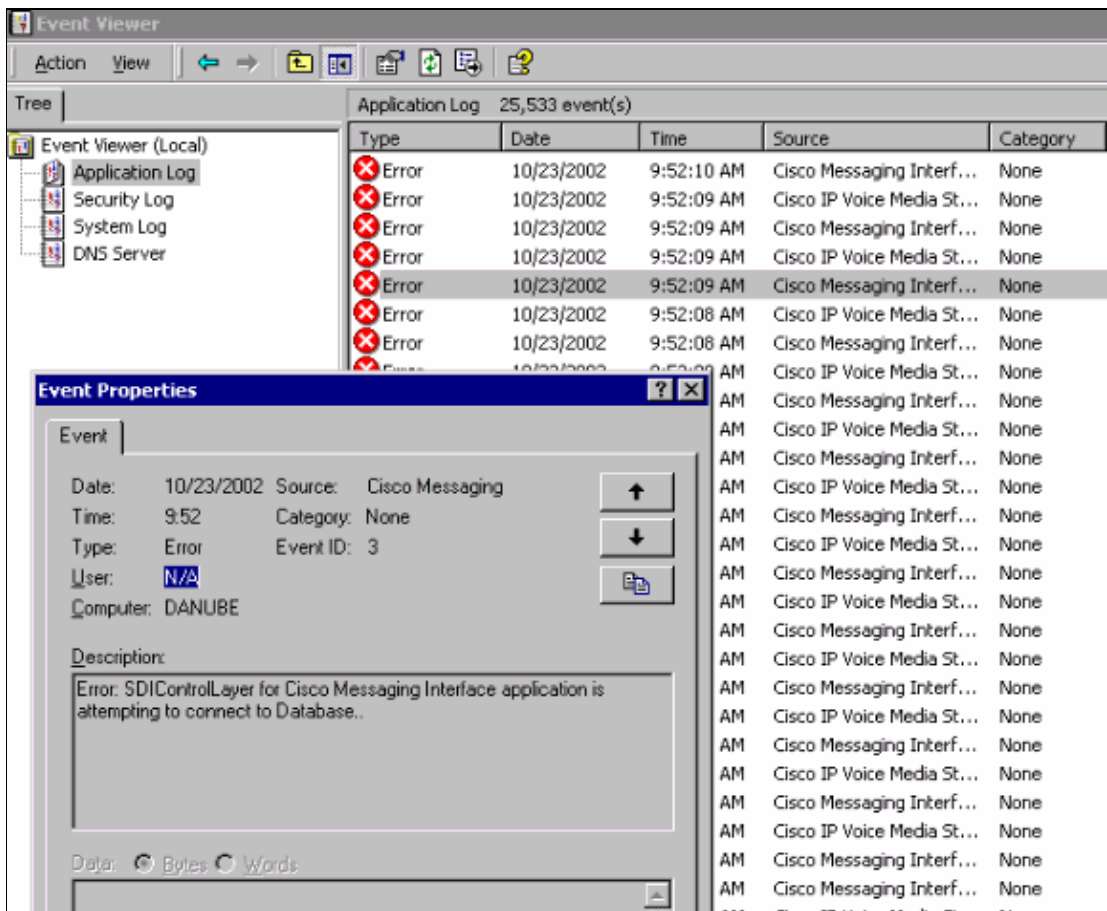
Cisco CallManager versions 3.1 and later are subject to these SQL–related problems:

- After you manually change the SQLSvc account, Cisco CallManager–related services and SQL–related services that start concurrently with the SQLSvc account do not start anymore, and you see Distributed Component Object Model (DCOM) errors in your event viewer. These three figures

provide an example:

- ◆ DCOM got error "Logon failure: unknown user name or bad password." and was unable to logon .\SQLSvc in order to run the server:
{4A783AD9-930D-4C6D-BAED-F9852EAAEB0D}
- ◆ Error: SDIControlLayer for Cisco Messaging Interface application is attempting to connect to database.
- ◆ Could not start the Cisco Music on Hold (MoH) Audio Translator service on local computer.
Error 1069: The error did not start due to a logon failure.





- An upgrade to Cisco CallManager version 3.2(2a) or 3.1(4a) can result in the same errors because the upgrade resets the SQLSvc password. This is described in more detail in Cisco CallManager Upgrade

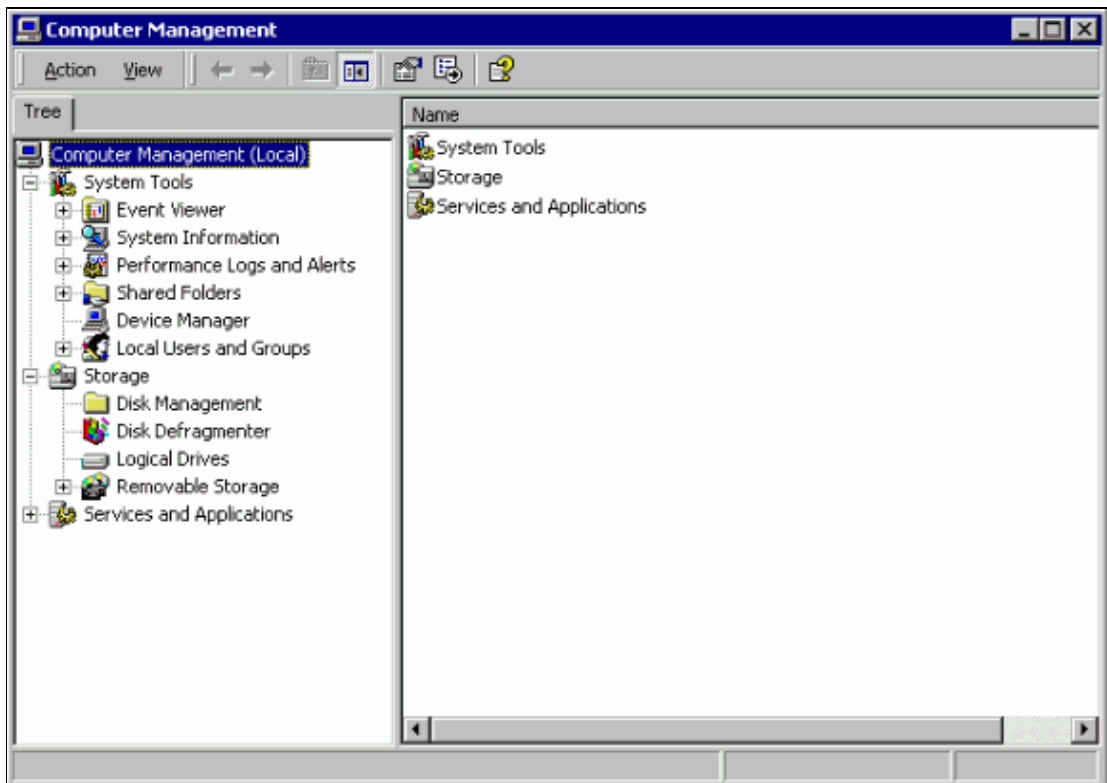
Changes the SQLSvc Password.

Solution 1

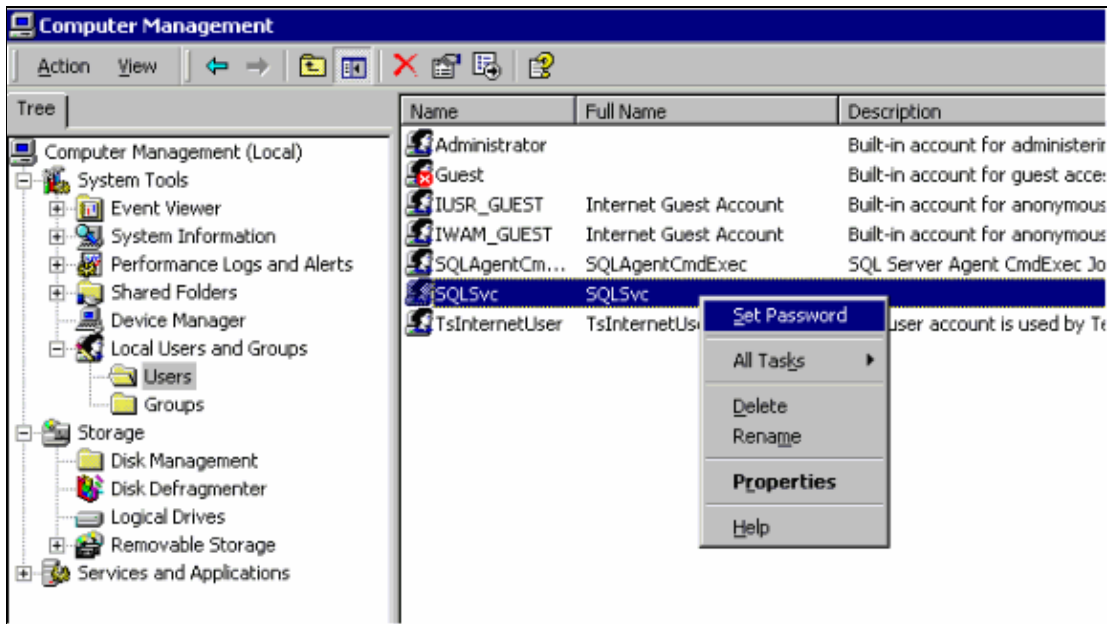
Verify the password for the SQLSvc user and for the services that use the SQLSvc account as described in Cisco CallManager Upgrade Changes the SQLSvc Password.

1. Select **Start > Programs > Administrative Tool > Computer Management**.

The Computer Management window displays.

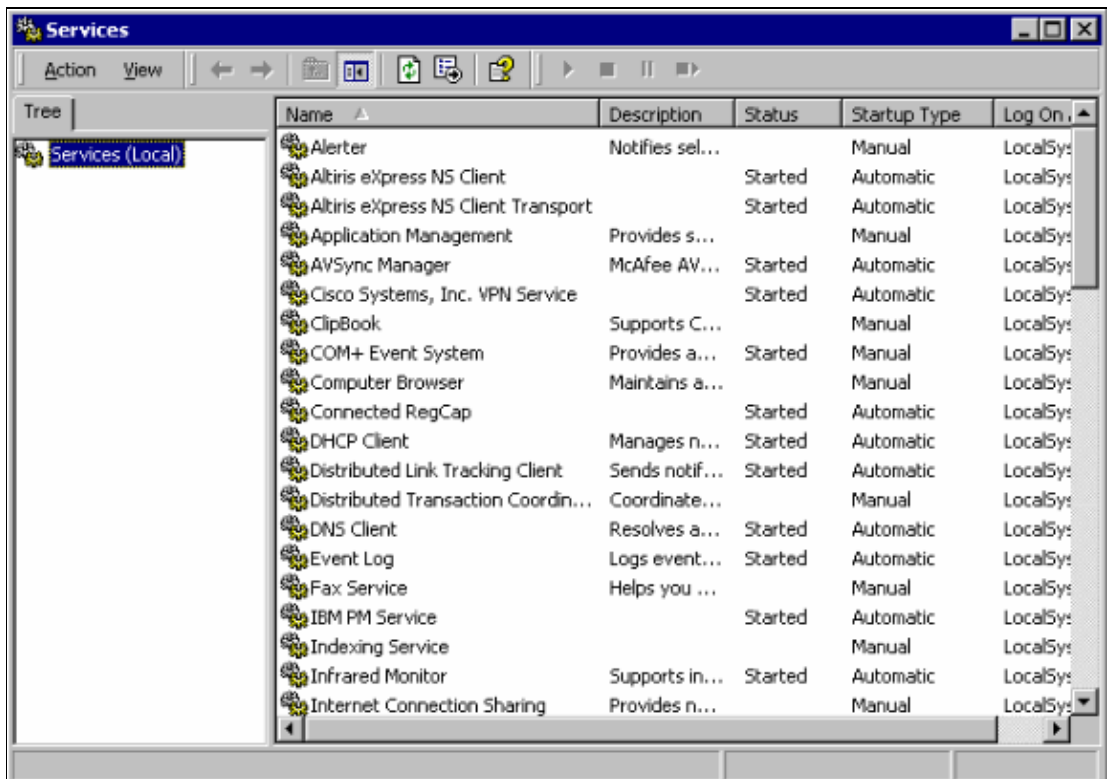


2. Select **System Tools > Local Users and Groups > Users**.
3. Among the Users select **SQLSvc user**. Right-click and choose **Set Password**.
4. Set the correct password.

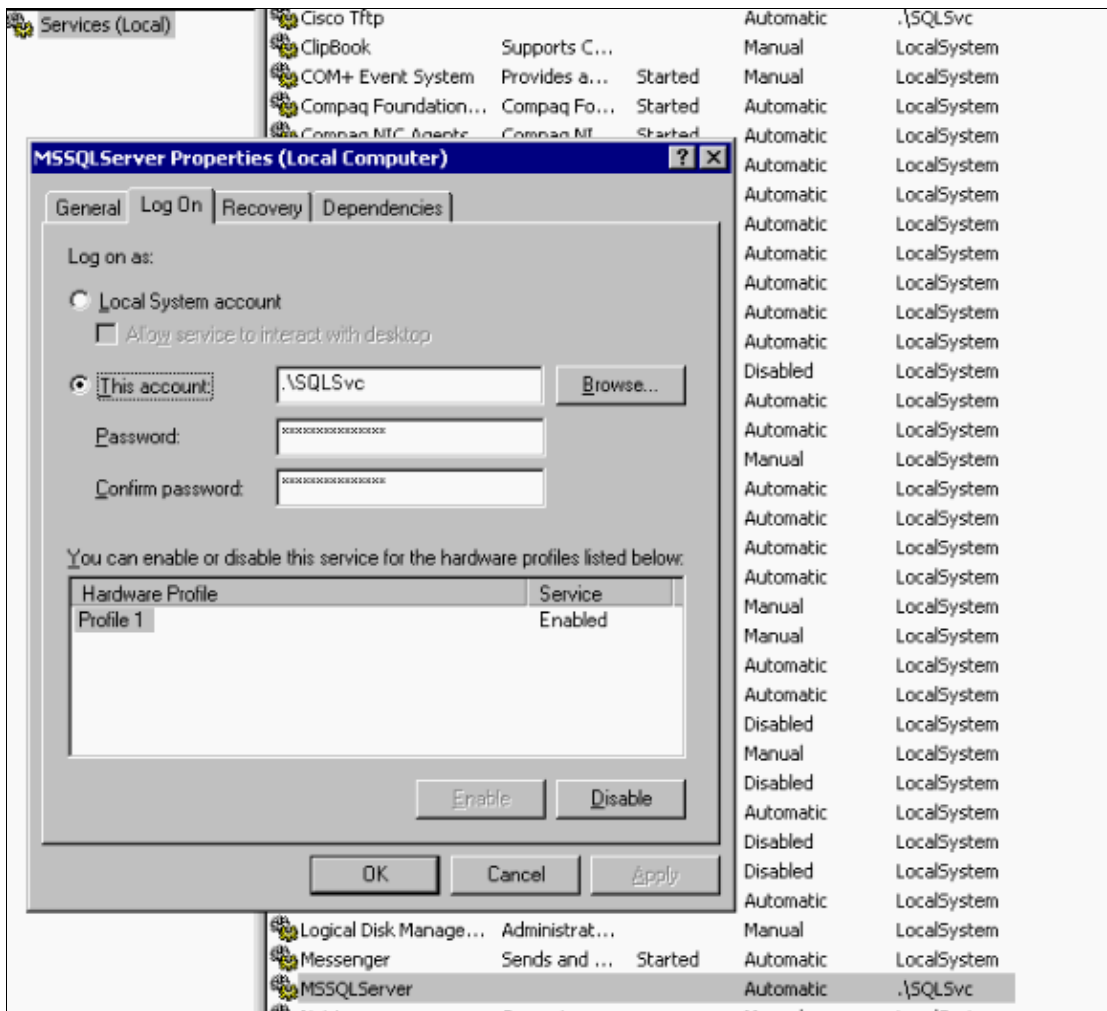


5. Select **Start > Programs > Administrative Tools > Services**.

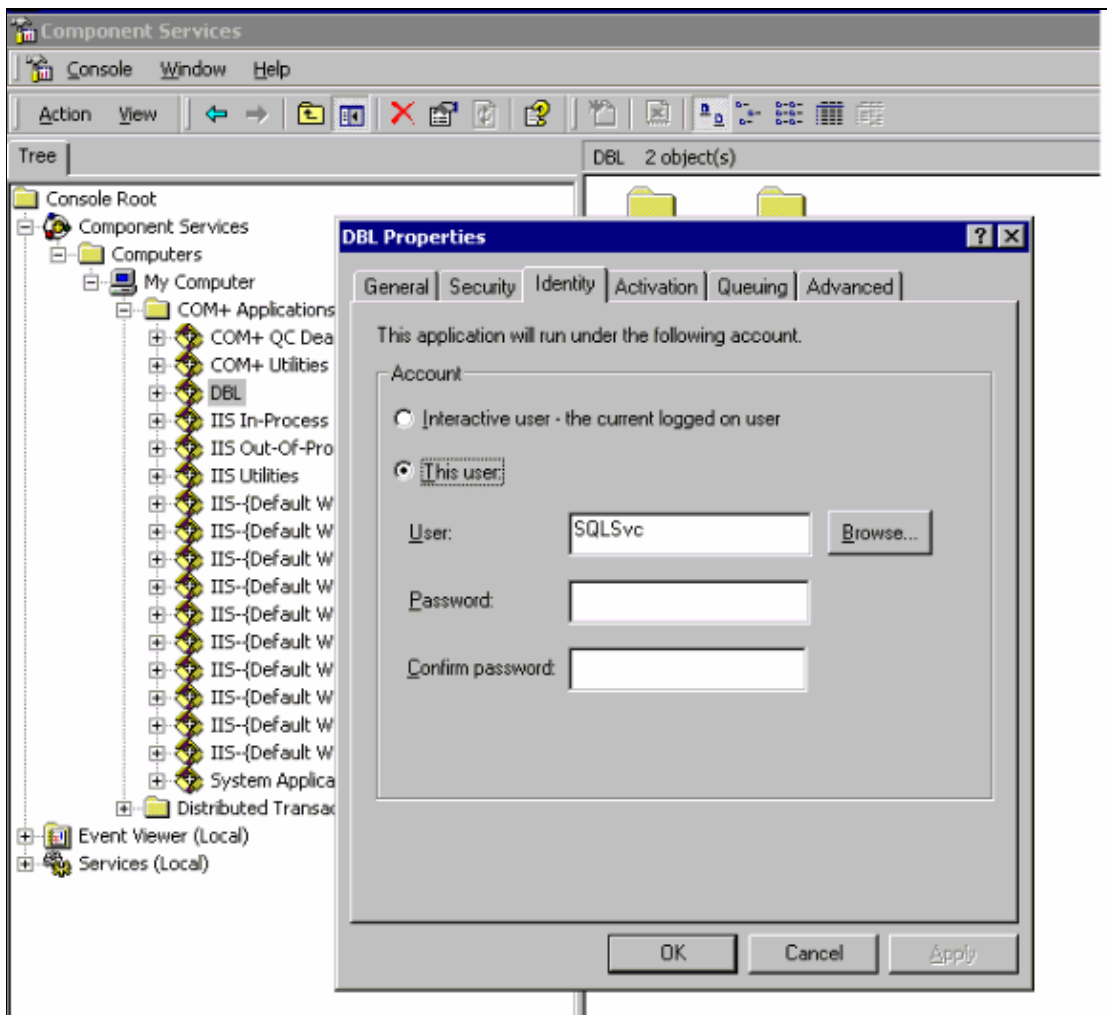
The Services window displays.



6. Right-click the service, select the **Log On** tab, select the **This account** radio button, and set the password in order to verify the password for all the services that use the SQLSvc account.



7. Select **Start > Programs > Administrative Tools > Component Services** to restart the service.
8. Select **Computer > My Computer > COM+ Application > DBL**.
9. Right-click **DBL**, select **Properties**, and then select the **Identity** tab.



10. Use the fields provided to select the correct password.
11. Right-click the service, select **Shut Down**, and then select **Start**.

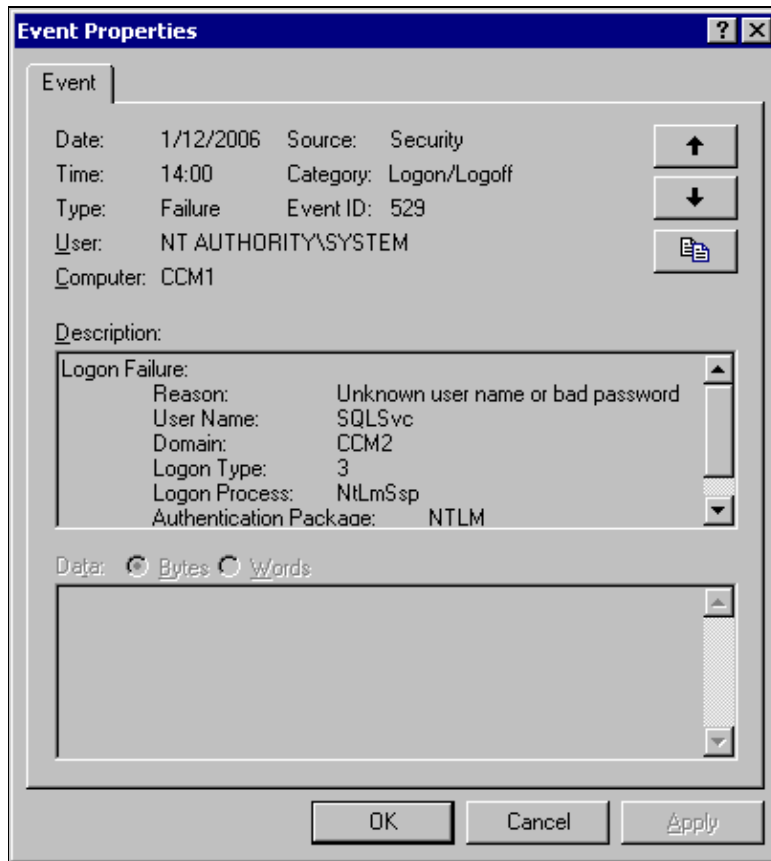
Cisco recommends that you reboot the server after you make the changes. If rebooting the server is not feasible, then restart SQL and Cisco CallManager-related services on that server.

Repeat steps 1 through 11 to verify the password on all the servers in the cluster.

Problem 2

Cisco CallManager-related services and SQL-related services that start concurrently with the SQLSvc account do not start anymore, and you see this security error in your event viewer, as this figure shows:

Unknown user name or bad password

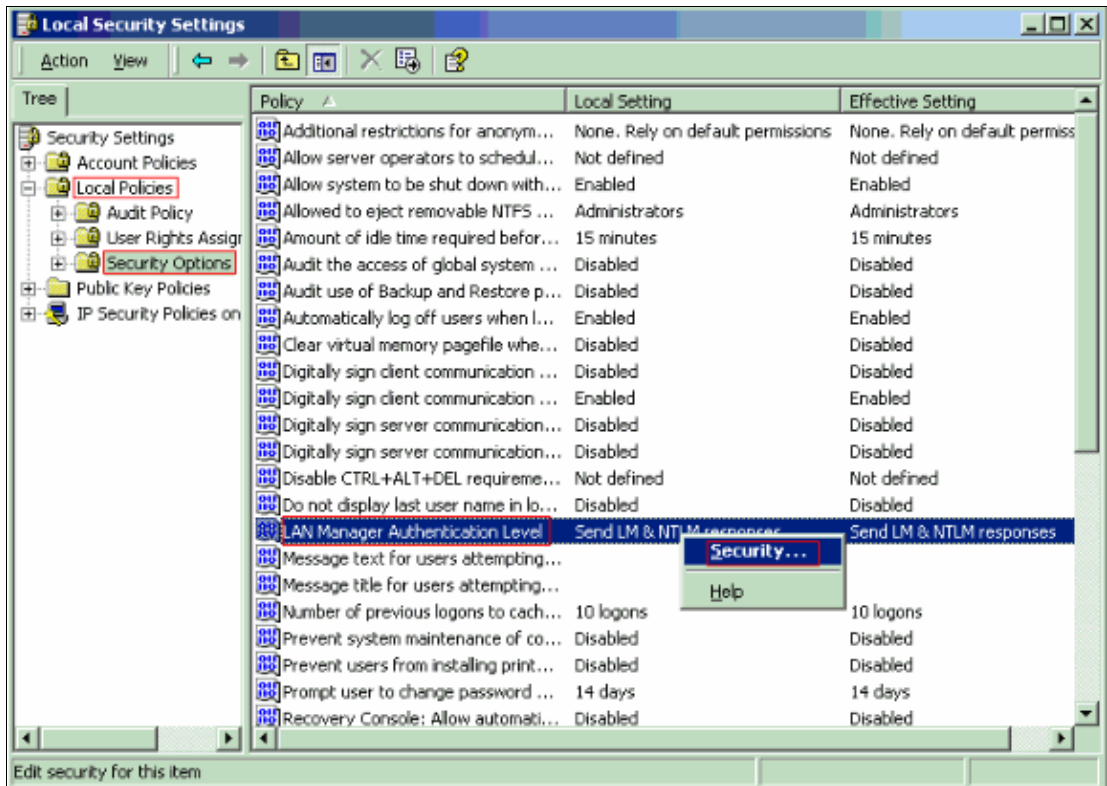


Solution 2

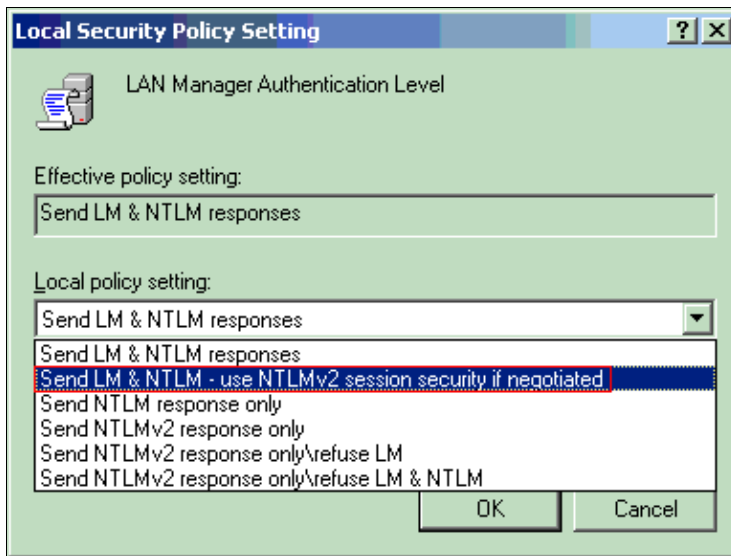
This error can be generated if the Network Security settings are changed in the Cisco CallManager servers. The LAN Manager authentication level for the Cisco CallManager server needs to be **Send LM & NTLM – use NTLMv2 session security if negotiated**.

Complete these steps to verify and change the authentication level:

1. Select **Start > Programs > Administrative Tools > Local Security Policy**.
2. In the Local Security Settings window select **Local Policies > Security Options > LAN Manager Authentication Level**.



3. Right-click on the policy and choose the **Security...** option.
4. In the Local Security Policy Setting window, choose the **Send LM & NTLM – use NTLMv2 session security if negotiated** value from the Local policy setting list.



5. Click **OK**.

Repeat steps 1 through 5 to verify the authentication level on all the servers in the cluster.

Refer to the Network Security: LAN Manager Authentication Level Microsoft article.

Related Information

- **Recovering an SQLSvc Account Password**
 - **CallManager Upgrade Changes the SQLSvc Password**
 - **Network Security: LAN Manager Authentication Level**
 - **Voice Technology Support**
 - **Voice and IP Communications Product Support**
 - **Recommended Reading: Troubleshooting Cisco IP Telephony**
 - **Technical Support & Documentation – Cisco Systems**
-

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Mar 20, 2006

Document ID: 27540
