Riverbed Technology, Inc.
680 Folsom Street
San Francisco, CA 94107
Phone 415.247.8800
Fax 415.247.8801
www.riverbed.com

Riverbed SteelCentral™ ADConnector 2.0 Release Notes

1 What's new in Version 2.0

Version 2.0 of the ADConnector application introduces support of Windows Server 2008 R2 and Windows Server 2008 Active Directory Domain Services. It is built upon the new Windows Event Log architecture included beginning with Windows Vista and Windows Server 2008.

Note that Windows Server 2003 and Windows Server 2000 are no longer supported by ADConnector 2.0. For these Windows Server versions, Mazu ADConnector 1.5[1] should be used.

2 Overview

The SteelCentral NetProfiler user identity feature relies on the Security Audit Events obtained from one or more Microsoft Active Directory Domain Controllers. This event data can be sent directly to the NetProfiler appliance from a Domain Controller or an Event Collector host. Riverbed provides the ADConnector service application to connect a Domain Controller or Event Collector to the NetProfiler.

The ADConnector application uses LDAP protocol to identify domain names and fetch user identity data. Therefore, ensure that there are no firewall rules in place that block LDAP port 389 or LDAPS port 636 between the ADConnector application and the Active Directory Domain Controller.

Beginning with Windows Vista and Windows Server 2008, the Windows Event Forwarding feature is shipped with Windows platforms. Event Collector[2] is a term used by Microsoft for the event collecting computer. The SteelCentral ADConnector service can send the collected event data from an Event Collector to the NetProfiler.

[1] Mazu ADConnector 1.5 is downloadable from NetProfiler Help system.
[2] This is NOT Audit Collection Services (ACS) in Microsoft System Center Operations Manager 2007.

2.1 Collected Events

SteelCentral ADConnector service reads the following Windows Security Audit Events from Windows Event Log and sends them to NetProfiler.

Category	Subcategory	Event ID	Message Summary
Account Logon	Credential Validation	4774	An account was mapped for logon.
Account Logon	Credential Validation	4775	An account could not be mapped for logon.
Account Logon	Credential Validation	4776	The domain controller attempted to validate the credentials for an account.
Account Logon	Credential Validation	4777	The domain controller failed to validate the credentials for an account.
Account Logon	Kerberos Authentication Service	4768	A Kerberos authentication ticket (TGT) was requested.
Account Logon	Kerberos Authentication Service	4771	Kerberos pre-authentication failed.
Account Logon	Kerberos Authentication Service	4772	A Kerberos authentication ticket request failed.
Account Logon	Kerberos Service Ticket Operations	4769	A Kerberos service ticket was requested.
Account Logon	Kerberos Service Ticket Operations	4770	A Kerberos service ticket was renewed.
Logon/Logoff	Logon	4624	An account was successfully logged on.
Logon/Logoff	Logon	4625	An account failed to log on.
Logon/Logoff	Logon	4648	A logon was attempted using explicit credentials.

For more information about these events, refer to:

- Security audit events for Microsoft Windows Server 2008 and Microsoft Windows Vista http://www.microsoft.com/downloads/details.aspx?FamilyID=82e6d48f-e843-40ed-8b10-b3b716f6b51b
- Security Audit Events for Windows 7 and Windows Server 2008 R2 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=3a15b562-4650-4298-9745-d9b261f35814

3 Prerequisites

Prior to starting the installation, the following conditions must be met.

- Your user account on the NetProfiler appliance is enabled for viewing user identity information.
- The target computer (Domain Controller or Event Collector) must be able to connect to TCP port 42999 on NetProfiler.
- If the ADConnector application is installed on the Event Collector, it must be able to connect to LDAP port 389 and LDAPS port 636 on the Active Directory Domain Controller.
- The target computer has Windows Installer version 3.1 or later.

- The target computer has .NET Framework 3.5 SP1 or later.
- The Audit Policy of the Active Directory Domain Controllers is set to:

  Audit account logon events: **Success** and **Failure**

Note: If the Failure audit is not enabled, NetProfiler will not be able to report failed login attempts. For more information about the Audit Policy, refer to:

- Audit Policy
  http://technet.microsoft.com/en-us/library/dd349800(WS.10).aspx

3.1 Event Collector

In addition to the above, when installing the SteelCentral ADConnector on an Event Collector,

- Event Forwarding must be enabled between the Domain Controllers and the Event Collector.

The configuration detail is beyond the scope of this document. Please refer to the appropriate Microsoft documentation. Here are a few useful links:

- Configure Computers to Forward and Collect Events
  http://technet.microsoft.com/en-us/library/cc748890.aspx
- Quick and Dirty Large Scale Eventing for Windows
  http://blogs.technet.com/b/otto/archive/2008/07/08/quick-and-dirty-enterprise-eventing-for-windows.aspx
- Forwarding Security Events from Windows XP, Server 2003, and Vista/Server 2008
  http://blogs.technet.com/b/otto/archive/2009/06/22/forwarding-security-events-from-windows-xp-server-2003-and-vista-server-2008.aspx

We recommend trying the Source computer initiated subscription described in Quick and Dirty Large Scale Eventing for Windows article with a Domain Controller being the source. After successful forwarding of Application and/or System events, you can proceed with adding “Network Service” to the “Event Log Readers” Local Security Group described in Forwarding Security Events from Windows XP, Server 2003, and Vista/Server 2008 article. Please make sure to reboot a Domain Controller after the group membership change.

A custom Event Forwarding Subscription XML file is included in the SteelCentral ADConnector installation package. It will be used to create a new push subscription.

4 Installation

Choose either “4.1 On Domain Controller” or “4.2 On Event Collector” method, not both. The installation on a Domain Controller is simpler; however it must be done as many times as the number of Domain Controllers. The installation on an Event Collector requires a few more steps, including planning of event collecting topology; however it requires no additional product installed on Domain Controllers and provides more flexible delivery paths.

Before proceeding, check this list:

- ❑ Network connectivity to NetProfiler appliance
- ❑ Windows Installer version 3.1 or later
- ❑ .NET Framework 3.5 SP1 or later
- ❑ Audit Policy of the Active Directory Domain Controllers
- ❑ Event Forwarding between the Domain Controllers and the Event Collector

4.1 On Domain Controller

Perform the following steps on each Domain Controller.

1. Log on as a Domain Administrator (member of **Domain Admins** or **Enterprise Admins** group).
2. Download the ADConnector.zip file from https://support.riverbed.com/content/support/software/steelcentral-npm/net-profiler/integration.html and unzip its contents.
3. Right-click ADConnector-x64.msi for 64-bit Windows or ADConnector-x86.msi for 32-bit Windows, then choose **Install**.
4. Answer the questions asked by the Setup wizard and follow the instructions until the installation completes.

4.2 On Event Collector

Perform the following steps on an Event Collector.

1. Log on as a Domain Administrator (member of **Domain Admins** or **Enterprise Admins** group).
2. Download the ADConnector.zip file from https://support.riverbed.com/content/support/software/steelcentral-npm/net-profiler/integration.html and unzip its contents.
3. Right-click ADConnector-x64.msi for 64-bit Windows or ADConnector-x86.msi for 32-bit Windows, then choose **Install**.
4. Answer the questions asked by the Setup wizard and follow the instructions until the installation completes.

5. Start Command Prompt as Administrator (Right-click on **Start > All Programs > Accessories > Command Prompt**, then choose **Run as administrator**).
6. CD to the ADConnector directory (by default "%ProgramFiles%\Riverbed\Cascade AD Connector").
7. Create a new Event Forwarding subscription by executing:
   ```
   wecutil cs Account-Logon.xml
   ```
8. Open the Config.xml file in Notepad, add the <reader query="ForwardedEvents.xml" /> element to the <configuration> element. Save and close.
9. Restart the ADConnector service by executing:
   ```
   sc stop "Riverbed Cascade AD Connector"
   sc start "Riverbed Cascade AD Connector"
   ```
   (Or Click **Server Manager** from the Quick Launch, and go to **Configure > Services**.)

Here is an example of Config.xml file change, before:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration xmlns="urn:xmlns:riverbed-com:cascade:identity">
 <servers>
  <server host="cascade-profiler.riverbed.com" />
 </servers>
</configuration>
```

and after:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration xmlns="urn:xmlns:riverbed-com:cascade:identity">
 <reader query="ForwardedEvents.xml" />
 <servers>
  <server host="cascade-profiler.riverbed.com" />
 </servers>
</configuration>
```

4.3 Unattended Mode Installation

For large scale deployment of the ADConnector to Domain Controllers, it is desirable to install it without the Setup Wizard UI. You can specify the NetProfiler hostname (or IP address) in the PROFILER property when starting msiexec in no UI mode. For example,

```
msiexec /qn /i ADConnector-x64.msi PROFILER=netprofiler.riverbed.com
```

5 Advanced Configuration

5.1 Multiple NetProfiler Appliances

It is possible to send event data to multiple NetProfiler appliances by adding a <server> element for each NetProfiler in the <servers> element of Config.xml file.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration xmlns="urn:xmlns:riverbed-com:cascade:identity">
 <servers>
  <server host="cascade-profiler.riverbed.com" />
  <server host="cascade-profiler2.riverbed.com" />
 </servers>
</configuration>
```

The SteelCentral ADConnector service must be restarted after editing the Config.xml file.

5.2 Rename Subscription ID

The Account-Logon.xml file in the ADConnector directory is used to create a source-initiated (push) Event Forwarding subscription. Its subscription ID is “Account Logon.” If the same subscription ID is already used on the Event Collector, you must edit the Account-Logon.xml file to rename it (in the <SubscriptionId> element).

```
<?xml version="1.0" encoding="UTF-8"?>
<Subscription xmlns="http://schemas.microsoft.com/2006/03/windows/events/subscription">
        <SubscriptionId>Account Logon</SubscriptionId>
        <SubscriptionType>SourceInitiated</SubscriptionType>
        <Description></Description>
                ...
        <Locale Language="en-US"/>
        <LogFile>ForwardedEvents</LogFile>
        <PublisherName>Microsoft-Windows-EventCollector</PublisherName>
                ...
</Subscription>
```

Its default destination is the ForwardedEvents logfile. If you set up a dedicated logfile for the forwarded audit events, you can change it in the <LogFile> element. If you change the destination, you must also edit the ForwardedEvents.xml file to change the Path attribute of the <Select> elements.

```
<QueryList>
  <Query Id="0" Path="ForwardedEvents">
    <Select Path="ForwardedEvents">
      *[System[(EventID &gt;= 4768) and (EventID &lt;= 4777)]]
    </Select>
    <Select Path="ForwardedEvents">
      *[System[EventID=4624 or EventID=4625 or EventID=4648]]
    </Select>
  </Query>
</QueryList>
```

6 Limitations

6.1 No IPv6 Support

If a domain member machine authenticates using an IPv6 connection, the ADConnector does not send the event to NetProfiler because IPv6 is not supported. The exception exists for the IPv4-Mapped IPv6 Address (defined in RFC 4291). The IPv4-Mapped IPv6 Address encodes the IPv4 address into the low-order 32 bits of the IPv6 address with the fixed prefix of 0:0:0:0:0:FFFF (the high-order 96 bits), such as ::ffff:10.38.8.86. When an event with the IPv4-Mapped IPv6 Address is seen, the ADConnector extracts the IPv4 address and sends the event to NetProfiler.

6.2 No non-English User Name Support

The ADConnector itself operates in Unicode and sends user names encoded in UTF-8 to NetProfiler. However, NetProfiler processes them as encoded in ASCII (English/US locale). Thus, it may misinterpret them or be unable to process them.

7 Troubleshooting

7.1 Reading the SteelCentral ADConnector log

The ADConnector logs its messages to the Application log. They can be viewed by the Windows Event Viewer UI (**eventvwr**) or **wevtutil** command line utility. To display the most recent 10 messages, run:

```
wevtutil qe Application
/q:"*[System/Provider/@Name=\"Riverbed Cascade AD Connector\"]" /rd:true /c:10
/f:text
```

The ADConnectorLog.xml file installed in the ADConnector directory provides another example to display warning and error messages.

7.2 Installation is blocked by the security policy

The Setup Wizard may fail in some secure environments because of a policy violation. For instance, Windows policy is set to deny a privilege elevation request automatically.

As a workaround, instead of clicking **Install**, perform the following steps:

1. Start Command Prompt as Administrator (Right-click **Start > All Programs > Accessories > Command Prompt**, then choose **Run as administrator**).
2. CD to the directory where the ADConnector.zip file was extracted.
3. Execute "**`msiexec /i ADConnector-x64.msi`**" for 64-bit Windows or "**`msiexec /i ADConnector-x86.msi`**" for 32-bit Windows.
4. Answer the questions asked by the Setup wizard and follow the instructions until the installation completes.

If the failure persists, please generate the detailed log with the /l option of msiexec and report it to Riverbed Support for the further analysis, for instance by running "**`msiexec /l*vx msi.log /i ADConnector-x64.msi`**".

7.3 ADConnector does not start

In the Application eventlog, the "Found no client certificate!" error message was left by the ADConnector service before stopping.

The ADConnector service communicates with the identityd daemon running on NetProfiler over the SSL connection (port 42999). The identityd process mandates a client certificate. The ADConnector service uses a suitable certificate found in the local machine certificate store. For instance:

```
C:\> certutil -store My
My
================ Certificate 0 ================
Serial Number: 70204cde00000000036b
Issuer: CN=RIVERBED, DC=riverbed, DC=com
 NotBefore: 1/1/2010 9:53 AM
 NotAfter: 1/1/2011 9:53 AM
Subject: CN=RIVERBED-DC.riverbed.com
Certificate Template Name (Certificate Type): Machine
Non-root Certificate
Template: Machine, Computer
Cert Hash(sha1): d8 04 33 c7 a3 b9 c8 48 f7 21 5c 87 35 84 28 7e 3a 4c 06 6e
  Key Container = d08375f4a7f01738882e58cbb5ca21a1_6c3d6b14-2253-4b1a-91e2-
e6b1440a456e
  Simple container name: le-Machine-3b5f5ac2-4507-4072-b996-2e77bc3cada9
  Provider = Microsoft RSA SChannel Cryptographic Provider
Private key is NOT exportable
Encryption test passed
CertUtil: -store command completed successfully.
```

If no suitable certificate is found, the ADConnector service does not start.

The recommended solution for this issue is to install a machine certificate by requesting it from your Certification Authority. (Start mmc Console, Certificate snap-in for Computer account. Select **Certificates > Personal > Certificates**. Then select **Action > All Tasks > Request New Certificate…**) This requires Active Directory Certificate Services running in your domain.

Another option is to generate a self-signed certificate for the ADConnector service. For that, start a Command Prompt as Administrator (Right-click **Start > All Programs > Accessories > Command Prompt**, then choose **Run as administrator**) and execute the GenSelfCert tool.

```
C:\> cd "%ProgramFiles%\Riverbed\Cascade AD Connector"
C:\Program Files\Riverbed\Cascade AD Connector> GenSelfCert.exe
Computer: AD-CONNECTOR
DNS:      ad-connector.riverbed.com
Subject:  CN=ad-connector,DC=riverbed,DC=com
DN:       CN=AD-CONNECTOR,CN=Computers,DC=riverbed,DC=com

Successfully created 'AD-CONNECTOR.pfx'
```

Do **NOT** install this certificate to the local machine certificate store. The ADConnector service will load a certificate from the %COMPUTERNAME%.pfx file if no certificate is found in the local machine certificate store.

7.4 No Security Audit Event logged on a Domain Controller

No Security Audit event (listed in "2.1 Collected Events") is logged in Domain Controller's Security log or no Failure audit is logged.

Make sure that the Audit Policy requirement is met. This Audit Policy requirement can be verified by the following command.

```
C:\> auditpol.exe /get /category:"Account Logon"
System audit policy
Category/Subcategory                      Setting
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success and Failure
  Kerberos Authentication Service         Success and Failure
  Credential Validation                   Success and Failure
```

It is recommended to set the Audit Policy from the Domain Controller's Group Policy so that when a new Domain Controller is deployed it gets set automatically. If the Group Policy is edited, make sure to apply it to Domain Controllers by running "**gpupdate /force**".

7.5 Cannot create a new Event Forwarding subscription

The wecutil create-subscription command fails with:

```
C:\...\Cascade AD Connector> wecutil cs Account-Logon.xml
Subscription Account Logon already exists. Error = 0x50.
The file exists.
```

See "5.2 Rename Subscription ID".

7.6 No Security Audit Event forwarded to an Event Collector

Security Audit events (listed in "0") are logged in Domain Controllers' Security log. However, no event is logged to Event Collectors' ForwardedEvents log.

On the Event Collector, verify that "**Account Logon**" subscription is enabled and source Domain Controllers are connected.

```
C:\> wecutil es
Account Logon

C:\> wecutil gr "Account Logon"

Subscription: Account Logon
        RunTimeStatus: Active
        LastError: 0
        EventSources:
                riverbed-dc.riverbed.com
                        RunTimeStatus: Active
                        LastError: 0
                        LastHeartbeatTime: 2010-05-27T12:00:05.346
```

The LastHeartbeatTime should be within 60 seconds from now. If no source Domain Controller is connected or the LastHeartbeatTime is over 60 seconds into the past, there is a connectivity issue or a misconfiguration of sources. Troubleshooting steps in Quick and Dirty Large Scale Eventing for Windows are good starting point to fix it.

If a source Domain Controller has never connected to the Event Collector (not listed in the EventSources), it is likely that Event Forwarding Group Policy is not configured on the source Domain Controller. On each Domain Controller, verify that the Event Collector is listed in SubscriptionManager key.

```
C:\> reg query
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\EventForwarding
\SubscriptionManager

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\EventForwarding
\SubscriptionManager
    1    REG_SZ    Server=ad-connector.riverbed.com
```

If you added "Network Service" to the "Event Log Readers" Local Security Group by following Forwarding Security Events from Windows XP, Server 2003, and Vista/Server 2008, make sure to reboot each Domain Controller and verify its membership.

```
C:\> net localgroup "Event Log Readers"
Alias name     Event Log Readers
Comment        Members of this group can read event logs from local machine
Members
-------------------------------------------------------------------------------
NT AUTHORITY\NETWORK SERVICE

The command completed successfully.
```