Cisco Prime Access Registrar 8.0.1 Release Notes

Cisco Prime Access Registrar (Prime Access Registrar) is a high performance, carrier class, 3GPP-compliant, 64-bit RADIUS/Diameter solution that provides scalable, flexible, intelligent authentication, authorization, and accounting (AAA) services.

Prime Access Registrar comprises a RADIUS/Diameter server designed from the ground up for performance, scalability, and extensibility for deployment in complex service provider environments including integration with external data stores and systems. Session and resource management tools track user sessions and allocate dynamic resources to support new subscriber service introductions.

Note Prime Access Registrar can be used with Red Hat Enterprise Linux (RHEL) 6.6/7.0/7.2/7.4 and CentOS 6.5 64-bit operating systems using kernel and Glibc.

Contents

This release note contains the following sections:

System Requirements

This section describes the system requirements to install and use the Prime Access Registrar software.

Table 1 lists the system requirements for Prime Access Registrar 8.0.1.

Cisco Systems, Inc.
www.cisco.com

Table 1 Minimum Hardware and Software Requirements for Prime Access Registrar Server

OS version	RHEL 6.6/7.0/7.2 CentOS 6.5
Model	X86
CPU type	Intel Xeon CPU 2.30 GHz
CPU Number	8
CPU speed	2.30 GHz
Memory (RAM)	8 GB
Swap space	10 GB
Disk space	1*146 GB
No: of Virtual Sockets	4
No: of Cores per Socket	2

Prime Access Registrar supports JDK versions 1.7 and 1.8 from release 7.3 onwards.

Co-Existence With Other Network Management Applications

To achieve optimal performance, Prime Access Registrar should be the only application running on a given server. In certain cases, when you choose to run collaborative applications such as a SNMP agent, you must configure Prime Access Registrar to avoid UDP port conflicts. The most common conflicts occur when other applications also use ports 2785 and 2786. For more information on SNMP configuration, see the "Configuring SNMP" section in the "Configuring Cisco Prime Access Registrar" chapter of the *Cisco Prime Access Registrar 8.0 Administrator Guide*.

New and Enhanced Features in Cisco Prime Access Registrar 8.0.1

Cisco Prime Access Registrar 8.0.1 provides the following features:

- Diameter Multiple Proxy Support, page 2
- Support for Packet Tracing per User, page 4
- Enhancements in Cisco Prime Access Registrar 8.0.1, page 4

Diameter Multiple Proxy Support

Prime Access Registrar supports Diameter client configurations in multiple proxy mode. As part of this functionality, client-based Diameter connections can be established from multiple peers with the same IP address but with different source ports and origin-hosts.

The Origin-Host AVP is of type Diameter Identity and must be present in all Diameter messages. This AVP is unique to a host and indicates the endpoint that originated the Diameter message.

When Prime Access Registrar gets a connection from any peer, initially Capabilities Exchange messages (CER-CEA) are exchanged with the client. These messages allow the discovery of peer's identity and its capabilities.

After successful Capabilities exchange with the client, Prime Access Registrar selects the exact client object from the CLI, based on the Origin-Host in CER packet.

A new attribute **EnableMultiProxyMode** is added to the Diameter client configuration to support this feature. To use this feature, you must configure at least two clients in multiple proxy mode, with the same source IP. Note the following:

- For all the clients configured in multiple proxy mode, the host name must be some name and not an IP address.
- The current implementation of this feature supports only Diameter TCP and TLS connections. It does not support Diameter Routing Agent (DRA) and SCTP connections.
- The maximum number of clients that can be configured in multiple proxy mode with the same IP is 15.
- All the clients configured in multiple proxy mode must have one and the same connection type; either TCP or TLS.

The following CLIs are sample configurations of two clients with same IP Address. **host-1** and **host-2** mentioned in the following samples are host names referring to the same IP address.

```
cli1/
        Name = cli1
        Description =
        Protocol = diameter
        EnableMultiProxyMode = TRUE
        HostName = host-1
        PeerPort = 3868
        Vendor =
        IncomingScript~ =
        OutgoingScript~ =
        AdvertisedHostName =
        UserLogEnabled =
        AdvertisedRealm =
        InitialTimeout = 1000
        MaxIncomingRequestRate = 0
        KeepAliveTime = 0
        AuthSessionStateInASR = State-Maintained
        SCTP-Enabled = FALSE
        TLS-Enabled = FALSE

    cli2/
        Name = cli2
        Description =
        Protocol = diameter
        EnableMultiProxyMode = TRUE
        HostName = host-2
        PeerPort = 3868
        Vendor =
        IncomingScript~ =
        OutgoingScript~ =
        AdvertisedHostName =
        UserLogEnabled = FALSE
        AdvertisedRealm =
        InitialTimeout = 1000
        MaxIncomingRequestRate = 0
        KeepAliveTime = 0
        AuthSessionStateInASR = State-Maintained
        SCTP-Enabled = FALSE
```

```
TLS-Enabled = FALSE
```

Support for Packet Tracing per User

Prime Access Registrar enables tracing packet flow for a single user or a particular set of users. You can also trace packet flow for an AVP. This feature is applicable for both RADIUS and Diameter packets and supports packet flows to remote servers as well.

Table 2 lists the CLI configuration options to support this feature.

Table 2 Configuration Options for Per-User Tracing

Action	Command	Example
To enable tracing for particular user	**perusertracing *<level>* User-Name=*<value>*** Where, trace level ranges from 1 to 5	***perusertracing 5 User-Name=bob***
To enable tracing for an AVP	**perusertracing <level> AVP-Name= <value>** **perusertracing <level> ~AVP-Name= <Pattern>** Where, trace level ranges from 1 to 5	***perusertracing 5 Origin-Host="epgchi01.03.epdg.epc.mnc300.mcc310.3gppnetwork.org"*** ***perusertracing 5 ~User-Name=Jane****
To remove tracing for particular user	**perusertracing 0 User-Name=<value>**	***perusertracing 0 User-Name=bob***
To remove tracing for any AVP	**perusertracing 0 AVP-Name=<value>**	***perusertracing 0 Origin-Host="epgchi01.03.epdg.epc.mnc300.mcc310.3gppnetwork.org"***
To remove all the traces	**perusertracing 0**	***perusertracing 0***

Enhancements in Cisco Prime Access Registrar 8.0.1

Following enhancements are available for Prime Access Registrar 8.0.1:

- Support for Replication via REST API—While configuring Prime Access Registrar via REST interface, supported objects will be replicated.
- Monitoring Diameter Stale Sessions in Prime Access Registrar, page 4
- Additional Counters for RAR Messages, page 5
- User Data Caching Option in Resource Manager, page 5

Monitoring Diameter Stale Sessions in Prime Access Registrar

Prime Access Registrar allows you to monitor the number of Diameter stale sessions. Table 3 lists the parameters introduced in Diameter Statistics (**dia-stats)** to support this feature.

Table 3 Dia-Stats Parameters

Parameter	Description	SNMP OID
cdbpLocalStatsTotalnumberofStaleSessions	Indicates the total number of Diameter stale sessions in Prime Access Registrar. The stale sessions will be released during the stale session removal process that runs at the specified purge time (/Radius/Advanced/DiameterStaleSessionPurgeTime).	.1.3.6.1.4.1.9.10.70.1.1.11.10
cdbpLocalStatsTotalnumberofSessions	Indicates the total number of Diameter sessions in Prime Access Registrar.	.1.3.6.1.4.1.9.10.70.1.1.11.9

Additional Counters for RAR Messages

Separate stats counters are introduced for Re-Auth-Request (RAR), Re-Auth-Answer (RAA) and failed RAR messages triggered during the session restoration process.

- cdbpPeerStatsRstRARsOut
- cdbpPeerStatsRstRAAsIn
- cdbpPeerStatsRstFailedRARs

You can monitor these counters in the Diameter Statistics (dia-stats) of the client before and after the restoration process.

Counter	SNMP OID
PeerStatsRstRARsOut	.1.3.6.1.4.1.9.10.70.1.1.14.1.98
PeerStatsRstRAAsIn	.1.3.6.1.4.1.9.10.70.1.1.14.1.99
PeerStatsRstFailedRARs	.1.3.6.1.4.1.9.10.70.1.1.14.1.100

User Data Caching Option in Resource Manager

During 3GPP call flows, Prime Access Registrar provides an option of caching all Access Point Names (APNs) or only a specific APN based on the CLI configuration in the resource manager.

The following CLIs show sample configurations of 3GPP and Session Cache resource managers with the new parameter:

```
[ //localhost/Radius/ResourceManagers/3ggp ]
    Name = 3ggp
    Description =
    Type = 3gpp
    EnableRegistrationFlow = TRUE
    EnableNon3GPPUserDataCaching = TRUE
    EnableSessionTermination = TRUE
    ReuseExistingSession = FALSE
    HSSProxyService = dia-proxy

[ //localhost/Radius/ResourceManagers/caching ]
    Name = caching
    Description =
    Type = session-cache
    OverwriteAttributes = FALSE
    EnableNon3GPPUserDataCaching = TRUE
    QueryKey = User-Name
```

```
PendingRemovalDelay = 10
AttributesToBeCached/
QueryMappings/
```

By default, the **EnableNon3GPPUserDataCaching** option is TRUE, which indicates that all APNs are cached. Set this option to FALSE, to cache only specific APN(s) based on the requirement.

Cisco Prime Access Registrar 8.0.1 Bugs

For information on a specific bug or to search all bugs in a particular Prime Access Registrar release, see Using the Bug Search Tool.

Fixed Anomalies in Cisco Prime Access Registrar 8.0.1.5

Table 4 lists the anomaly fixed in Prime Access Registrar 8.0.1.5 release.

Table 4 Fixed Anomaly in Prime Access Registrar 8.0.1.5

Bug	Description
CSCvo82754	Agent Server stopped working during Nessus vulnerability scanner. **PSIRT Evaluation** The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels. If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

Fixed Anomalies in Cisco Prime Access Registrar 8.0.1.4

Table 5 lists the anomaly fixed in Prime Access Registrar 8.0.1.4 release.

Table 5 Fixed Anomaly in Prime Access Registrar 8.0.1.4

Bug	Description
CSCvr25357	Reactivation not happening when the diameter connection is closed for the remote server randomly.

Fixed Anomalies in Cisco Prime Access Registrar 8.0.1.3

Table 6 lists the enhancements done in Prime Access Registrar 8.0.1.3 release.

Table 6 Enhancements in Prime Access Registrar 8.0.1.3

Bug	Description
CSCvp97185	Cisco Prime Access Registrar additional traps implementation for server monitor. For more information, see Additional Traps for Server Monitor.
CSCvp95166	Cisco Prime Access Registrar SSL connection handler enhancement for better resilience. For more information, see SSL Connection Handler.
CSCvp99977	TCP Options default values update in Radius-TLS Client for Cisco Prime Access Registrar. For more information, see TCP Option Default Values.

Fixed Anomalies in Cisco Prime Access Registrar 8.0.1.2

Table 7 lists the anomalies fixed in Prime Access Registrar 8.0.1.2 release.

Table 7 Fixed Anomalies in Prime Access Registrar 8.0.1.2

Bug	Description
CSCvn52619	High CPU utilization in Radius-TLS happens when SSL related error occurs while trying to establish connection.

Fixed Anomalies in Cisco Prime Access Registrar 8.0.1.1

Table 8 lists the anomalies fixed in Prime Access Registrar 8.0.1.1 release.

Table 8 Fixed Anomalies in Prime Access Registrar 8.0.1.1

Bug	Description
CSCvk26579	Backing store timing issue while deleting or accessing session record.
CSCvk41405	Prime Access Registrar stops working when extended-EAP is used with proxy service for a radius request without an IMSI.
CSCvk45227	MCD lock manager process keeps running even after Prime Access Registrar stops.
CSCvk66242	SSL disconnection happens frequently with different versions of TLS client.
CSCvk73771	REST Error when POD is initiated to release sessions.

Additional Traps for Server Monitor

CPAR supports Server Monitoring using which High and Low TPS thresholds can be monitored. For more details, see the *Cisco Prime Access Registrar User Guide, Cisco Prime Access Registrar Administrator Guide*.

A new attribute ServerMonitorAltApproach is introduced in aregcmd CLI under //localhost/Radius/Advanced. When SNMP is enabled, this attribute to set to true, and TPSHighThreshold, TPSLowThreshold, and ServerMonitorLogFreqInsecs in //localhost/Radius/Advanced/ServerMonitor are set to non zero values the four traps will be sent by Prime Access Registrar server in the following conditions:

- If the incoming TPS is maintained above configured TPSHighThreshold for a steady state period of five minutes, Prime Access Registrar sends the carTPSCapacityFull trap.
- If the incoming TPS is maintained below configured TPSLowThreshold for a steady state period of five minutes, Prime Access Registrar sends the carTPSCapacityNotFull trap.
- After reaching above TPSHighThreshold, if the incoming TPS decreases below TPSHighThreshold, Prime Access Registrar sends carTPSCapacityFullResetTrap trap.
- After reaching below TPSLowThreshold, if the incoming TPS increases above TPSLowThreshold, Prime Access Registrar sends carTPSCapacityNotFullResetTrap trap.

The traps have the following MIB objects.

Table 9 Trap MIB Objects

Trap Name	Object	Description
carTPSCapacityFullResetTrap	carNotifTPSHighThreshold	Indicates the maximum limit of the TPS of the Prime Access Registrar server.
	carNotifTPSLowThreshold	Indicates that the minimum limit of the TPS of the Prime Access Registrar server.
	carServerTPSUsage	Indicates the current TPS usage of the Prime Access Registrar server.
carTPSCapacityNotFullResetTrap	carNotifTPSHighThreshold	Indicates the maximum limit of the TPS of the Prime Access Registrar server.
	carNotifTPSLowThreshold	Indicates that the minimum limit of the TPS of the Prime Access Registrar server.
	carServerTPSUsage	Indicates the current TPS usage of the Prime Access Registrar server.

Note When ServerMonitorAltApproach attribute is set to TRUE, the TPSLowThreshold, TPSHighThreshold, and ServerMonitorLogFreqInsecs in server monitor configuration should be greater than zero. However; the lowest value for the TPSLowThreshold is one and TPSHighThreshold value should be higher than the TPSLowThreshold value.

An example configuration for the TPS monitoring includes:

```
--> cd /r/advanced/servermonitor/

    [ //localhost/Radius/Advanced/ServerMonitor ]
    TPSHighThreshold = 80
    TPSLowThreshold = 1
    SigtranTPSHighThrehold = 0
    SigtranTPSLowThreshold = 0
    SMHighThreshold = 0
    SMLowThreshold = 0
    SigtranSMHighThreshold = 0
    SigtranSMLowThreshold = 0
    ServerMonitorLogFreqInsecs = 10
    Set /Radius/Advanced/ServerMonitorAltApproach TRUE
```

SSL Connection Handler

SSL connection handler has been enhanced for better resilience. Changes include:

- The parallel thread handling mechanism that is already available for established TLS connection has been extended to the SSL connection establishment phase itself.
- A socket receive time out has been introduced before SSL accept in order to have a mechanism to close the SSL connection in the event of any problem during connection establishment.
- A configurable parameter called SocketReceiveTimeout has been introduced with a default value of five seconds for the socket receive timeout.

An example configuration includes:

```
Name = host1
 Description =
 Protocol = radius-tls
 IPAddress = host1
 SharedSecret = <encrypted>
 Type = NAS
 Vendor =
 IncomingScript~ =
 OutgoingScript~ =
 NetMask =
 EnforceTrafficThrottling = TRUE
 MaximumTLSConnections = 50
 SocketReceiveTimeout = 5
 RTLSOptions/
     PrivateKeyPassword =
     ServerCertificateFile = /cisco-ar/pki/server-cert.pem
     ServerKeyFile = /cisco-ar/pki/server-key.pem
     CACertificateFile = /cisco-ar/pki/root-cert.pem
     CACertificatePath = /cisco-ar/pki
     PeerVerificationMode = Optional
     VerificationDepth = 4
     EnableAutoChaining = True
 TCPOptions/
     KeepAliveIntervalTime = 60
     TCPConnectionIdleTime = 3600
     KeepAliveMaxtries = 5
[ //localhost/Radius/Clients ]
```

TCP Option Default Values

In /radius/clients/ under TCP Options of RADIUS-TLS type client default values for the TCP Keep Alive parameters are modified as:

```
[ //localhost/Radius/Clients/123/TCPOptions ]
KeepAliveIntervalTime = 60
TCPConnectionIdleTime = 3600
KeepAliveMaxtries = 5
```

KeepAliveIntervalTime and TCPConnectionIdleTime are measured in seconds.

Using the Bug Search Tool

Use the Bug Search tool (BST) to get the latest information about Cisco Prime Access Registrar bugs. BST allows partners and customers to search for software bugs based on product, release, and keyword, and it aggregates key data such as bug details, product, and version.

BST allows you to:

- Quickly scan bug content
- Configure e-mail notifications for updates on selected bugs
- Start or join community discussions about bugs
- Save your search criteria so you can use it later

When you open the Bug Search page, check the interactive tour to familiarize yourself with these and other Bug Search features.

Step 1 Log into the Bug Search Tool.

a. Go to https://tools.cisco.com/bugsearch.

b. At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 2 To search for a specific bug, enter the bug ID in the Search For field and press **Return**.

Step 3 To search for bugs in a particular release:

a. In the Search For field, enter the product name and the release version, e.g. Cisco Prime Access Registrar 8.0.1, and press **Return**. (Leave the other fields empty.)

b. When the search results are displayed, use the filter and sort tools to find the types of bugs you are looking for. You can search for bugs by severity, by status, how recently they were modified, according to the number of support cases associated with them, and so forth.

Related Documentation

For a complete list of Cisco Prime Access Registrar documentation, see the *Cisco Prime Access Registrar 8.0 Documentation Overview*.

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.