



Avaya Aura™ Communication Manager

Beschreibung der Änderungen für die Version 5.2.1

03-603443DE
Ausgabe 1
November 2009

Alle Rechte vorbehalten.

Hinweise

Es wurden angemessene Anstrengungen unternommen, um sicherzustellen, dass die in diesem Dokument enthaltenen Informationen vollständig und korrekt sind. Avaya Inc. kann jedoch keine Haftung für eventuelle Fehler übernehmen. Änderungen und Korrekturen der in diesem Dokument enthaltenen Informationen werden gegebenenfalls in zukünftigen Versionen aufgenommen. Der in diesem Dokument enthaltenen Informationen werden gegebenenfalls in zukünftige Versionen aufgenommen.

Vollständige Supportinformationen finden Sie im Gesamtdokument. *Avaya Support Notices for Hardware Documentation (Avaya-Supporthinweise zur Hardwaredokumentation)*, Dokumentnummer 03-600759.

Dieses Dokument finden Sie, indem Sie auf der Avaya-Website unter <http://www.avaya.com/support> in das Suchfeld die Dokumentnummer eingeben.

Haftungsausschluss für die Dokumentation

Avaya Inc. haftet für keine Änderungen, Ergänzungen oder Streichungen der ursprünglich veröffentlichten Fassung dieser Dokumentation mit Ausnahme der durch Avaya vorgenommenen Änderungen, Ergänzungen und Streichungen. Kunde und/oder Endnutzer erklären sich einverstanden, Avaya, die Agenten, Angestellten und Beschäftigten von Avaya im Falle von Forderungen, Rechtsstreitigkeiten, Ansprüchen und Urteilen auf der Grundlage von oder in Verbindung mit nachträglichen Änderungen, Ergänzungen oder Streichungen in dieser Dokumentation zu entschädigen und von jeglicher Haftung freizustellen, insoweit diese Änderungen, Ergänzungen oder Streichungen vom Kunden oder Endnutzer vorgenommen worden sind.

Haftungsausschluss für Links

Avaya Inc. haftet nicht für die Inhalte oder die Verlässlichkeit von verknüpften Websites, auf die an anderer Stelle in dieser Dokumentation verwiesen wird und unterstützt nicht notwendigerweise die Produkte, Dienstleistungen oder Informationen dieser Websites. Wir können nicht garantieren, dass diese Links jederzeit funktionieren, und wir haben keinen Einfluss auf die Verfügbarkeit dieser Websites.

Garantie

Avaya Inc. gewährt eine eingeschränkte Garantie auf dieses Produkt. Informationen über die Bedingungen der eingeschränkten Garantie finden Sie in Ihrem Kaufvertrag. Darüber hinaus finden Sie die normalen Garantiebedingungen von Avaya sowie Informationen über den während der Garantiezeit angebotenen Support für dieses Produkt auf der Avaya Support-Website: <http://www.avaya.com/support>

Urheberrecht

Das Produkt ist urheberrechtlich und durch andere Gesetze zum Schutz der Eigentümerrechte geschützt, es sei denn, es wurde ausdrücklich eine davon abweichende Regelung getroffen. Unbefugte Vervielfältigung, Weiterleitung oder Nutzung kann unter dem geltenden Recht straf- oder zivilrechtlich verfolgt werden.

Kontakt zum Support von Avaya

Avaya stellt Telefonnummern bereit, unter denen Sie Hilfestellung bei technischen Problemen oder Fragen zum Produkt erhalten. In den Vereinigten Staaten erreichen Sie den Support unter der Telefonnummer 1-800-242-2121. Weitere Support-Telefonnummern finden Sie auf der Support-Website von Avaya unter: <http://www.avaya.com/support>

Inhalt

Kapitel 1: Communication Manager Änderungen.....	7
14xx-Unterstützung mit Firmware-Download.....	7
Unterstützung der Avaya 14xx Digitaltelefone.....	7
Anforderungen für Firmware-Download.....	8
Rauschsignalunterstützung.....	9
RFC 3389 Rauschsignal.....	9
Communication Manager Aktualisierungs- und Migrationspfade.....	9
Server-Migrationspfad für Communication Manager Version 5.2.1.....	9
Bei Aktualisierungen unterstützte Server (nach Version).....	12
Kernel-Austausch.....	13
Info über Kernel-Ersatz.....	13
Kernel-Austausch mit System Management Interface.....	14
Kernel-Austausch mit Linux-Befehlen.....	19
Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer.....	22
Detaillierte Beschreibung von Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer.....	22
Firmware-Anforderungen für Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer.....	23
Anrufbearbeitungsszenarien.....	23
Verwaltung von Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer.....	25
Bedingungen für Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer.....	27
Interaktionen für Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer.....	28
Standortparameter.....	31
Systemparameter OCM-Ruftonklassifizierung.....	32
Connection Manager Ablehnungsereignisse.....	33
Spezialanwendung, Aktivierungsprozess.....	33
Kapitel 2: Avaya-Mediengateways, Änderungen.....	35
G450 - erhöhte Kapazität.....	35
show voip-parameters.....	35
MP20 - erhöhte Kapazität.....	36
Avaya G430 CLI-Befehle.....	36
Avaya G450 CLI-Befehle.....	40
ARP-Spoofing-Schutz.....	43
ip arp inspection.....	43
Protokollerweiterungen.....	44
power-down reset.....	46
reset power-down.....	46
Kapitel 3: SES-Änderungen.....	49
Installation des Avaya S8800 Servers für SES.....	49
Migration von S8500 und S8510 Servern zum S8800 Server.....	49
SES Mixed-mode Trusted Host Interface.....	49
Kapitel 4: Communication Manager Messaging - Änderungen.....	51
Installation von Avaya Aura™ Communication Manager Messaging auf einem S8800 Server.....	51
Neue Serverunterstützung für Communication Manager Messaging.....	51
Installation von Communication Manager Messaging.....	51
Sicheres Real-Time Transport Protocol (RTP).....	52
Überblick.....	52
Anmeldung beim Communication Manager-Server mit PuTTY.....	52

Zugriff auf den Communication Manager Server.....	52
Ändern von Kundenoptionen, um Medienverschlüsselung zu ermöglichen.....	53
Ändern von Signalisierungsgruppe, um Medienverschlüsselung zu ermöglichen.....	53
Einrichten des IP-Codecsatzes.....	54
Einrichten des SRTP-Typs auf der Communication Manager Messaging Verwaltungswebschnittstelle.....	54
Neustarten der Messaging-Anwendung.....	54
Aktivieren der Medienverschlüsselung für das Gateway.....	55
Zugriff auf Messaging für alle Nicht-SRTP kompatiblen Endpunkte zulassen.....	55
Aktualisieren von Avaya Aura™ Communication Manager Messaging.....	55
Aktualisieren von Communication Manager R5.1.x auf Communication Manager Messaging R5.2.1 auf einem S85XX Server.....	55
Aktualisieren von Communication Manager von R5.1 auf R5.2.1.....	56
Installation von Communication Manager Messaging R5.2.1.....	56
LDAP (Lightweight Directory Access Protocol).....	57
Überblick.....	57
Verbinden zu LDAP.....	57
LDAP-Prozesse.....	57
Statusüberprüfung der LDAP-Prozesse.....	58
Login-Profilinfrastruktur.....	58
Überblick.....	58
Erstellen eines Benutzer-basierten Profils.....	59
Zuweisen eines Profils zu einem Benutzer.....	59
Sichern und Wiederherstellen von Communication Manager Messaging-Daten.....	60
Überblick.....	60
Sichern von Communication Manager Messaging-Daten.....	60
Aktualisierungen von Dokumentation und Verfahren für Communication Manager Messaging R5.2.....	62
Ändern der Systemparameter – Weiterleitung.....	62
Ändern der Berechtigungsklasse.....	62

Kapitel 5: Communication Manager Installation auf S8800 Server.....63

Installation und Konfiguration von Avaya Aura™ Communication Manager.....	63
Überblick.....	63
Installation von Communication Manager.....	63
Erhöhen und Verringern der Verfügbarkeit des S8800 Servers.....	64
Konfiguration des Servers.....	64
Überwachung des Status des S8800 Server.....	65
Zugriff auf die Webseite „Configure Health Monitor“ (Statusüberwachung konfigurieren).....	65
Konfiguration von Communication Manager und Serverstatusparametern.....	66
S8800 Ethernet-Portzuordnungen.....	66
Verbesserungen der Softwaredoppelung.....	67
IP-Schnittstelle für H.248-Gateways.....	68
Prozessor-Ethernet-IP-Schnittstelle.....	68
Zuweisen der IP-Adresse zu Prozessor-Ethernet.....	68
Aktivierung von Prozessor-Ethernet.....	69
Zuweisen der IP-Adresse für Prozessor-Ethernet auf der System Management-Schnittstelle.....	69
Konfiguration von Secure Access Link (SAL).....	70
Konfigurieren von SAL-Gateway.....	70
Postinstallation.....	70
Aktivieren von Alarm an INADS über SAL.....	70
Installationsüberprüfung.....	70
Verbindung zum Server mit SAL.....	70

Kapitel 6: Hardware.....71

Digitaltelefone der Serien Avaya 14xx.....	71
Avaya S8800 Server - Übersicht.....	72
Einleitung.....	72
Kapitel 7: Dokumentations- und Verfahrensaktualisierungen.....	73
Administration für das Avaya G450 Media Gateway.....	73
DHCP-Server CLI-Konfiguration.....	73
Administrator Guide.....	73
Avaya Site Administration.....	74
Telefonfunktionstasten.....	74
Funktionsbeschreibung und Implementierung.....	74
Verwaltung von Nebenstelle zu Mobiltelefon.....	74
Bridged Call Appearance (Interaktionen für Leitungstastenkopie).....	75
Interaktionen für Whisper Paging.....	75
Hardwarebeschreibung und -übersicht.....	75
TN791 „Analog Guest Line“ (Gast-Analogleitung) – 16 Ports.....	75
Avaya S8800 Server.....	76
Screen Reference.....	82
AAR und ARS Digit Analysis Table (Ziffernanalysetable).....	82
AAR- und ARS-Ziffernumsetzungstabelle.....	82
BCMS/VuStats Service-Level.....	83
Nur-Nebenstellenkennzeichen für Team-Taste auf 96xx H.323-Terminals.....	83
Externes Klingelzeichen für Anrufe mit Amtsleitungen.....	83
Hunt Group (Sammelgruppe).....	84
Ankommende Dialog-Prüfschleifen.....	85
ISDN Numbering Umwandlung der Calling Party Number (CPN - Rufnummer des Anrufers) für Tandem- verbindungen.....	86
Standortparameter.....	86
off-pbx-telephone station-mapping.....	87
Timer der Trennung von abgehenden Amtsverbindungen (Minuten).....	88
Refresh Terminal Parameters Access Code.....	88
Gemeinsam genutzte UUI-Funktionsprioritäten.....	88
Station (Nebenstelle).....	90
Survivable ARS Analysis Table (Ausfallsichere ARS-Ziffernanalysetable).....	91
Trunk Group.....	92
Uniform Dial Plan Table (Rufnummernplan-Tabelle).....	92
Verwenden Sie „Trunk COR“ für die Unterbrechung der ausgehenden Amtsleitung.....	93
„VDN Override for ISDN Trunk ASAI Messages“ (VDN-Umgehung für ASAI-Nachrichten über ISDN- Amtsleitungen).....	93
Index.....	95

Kapitel 1: Communication Manager Änderungen

Dieses Kapitel beschreibt die Funktionen und Erweiterungen der Version 5.2.1 von Avaya Aura™ Communication Manager, die auf Avaya S8xxx Servern mit zugehörigen Avaya Media Gateways läuft.

Die Erweiterungen für Call Center 5.2.1 werden behandelt in *What's New for Avaya Aura™ Call Center 5.2.1*, 07-602633.

14xx-Unterstützung mit Firmware-Download

Unterstützung der Avaya 14xx Digitaltelefone

Communication Manager liefert Unterstützung der Avaya 14xx Digitaltelefone. Sie können diese Telefone in vorhandenen Systemen einsetzen, wenn Sie diese konfigurieren oder an die entsprechenden Typen der Avaya 24xx Digitaltelefone anpassen. Die Avaya 14xx Digitaltelefone werden später nativ unterstützt.

Die Avaya 14xx Digitaltelefone (1408 und 1416) sind Firmware-downloadfähig. Die Funktion Firmware-Download ermöglicht es Ihnen, die Avaya 14xx Digitaltelefone zu verwalten und zu warten. Wenn Sie das Avaya 14xx Digitaltelefon als Avaya 24xx Digitaltelefon umbenennen und verwalten, ermöglicht Communication Manager den Firmware-Download auf das Avaya 14xx Digitaltelefon (Nebenstelle).

Hinweis:

Es ist sehr zu empfehlen, dass Sie vor Hinzufügen eines 14xx Nebenstellentyps den SAT-Befehl `change alias station` ausführen (für das Aliasing der neuen Nebenstellentypen). Sie können 1408 in 2410 und 1416 in 2420 umbenennen. Danach können Sie die Befehle Hinzufügen, Ändern, Entfernen oder Auflisten über die 14xx Nebenstellentypen ausführen, was es Ihnen auch ermöglicht, alle Nebenstellen aufzulisten, die Sie mit diesen Nebenstellentypen hinzugefügt haben. Beispiele: Auflisten von Nebenstellentyp 1408.

Anforderungen für Firmware-Download

Communication Manager unterstützt Firmware-Download an die Avaya 14xx Digitaltelefone, wenn der Telefentyp, der einen Download anfragt, als Avaya 2410 oder 2420 Digitaltelefon verwaltet oder benannt wurde. Communication Manager unterstützt Firmware-Download an die 1408 und 1416 Digitaltelefone in der gleichen Weise wie die Avaya 2410 und 2420 Digitaltelefone. Die Telefentypen 1408 und 1416 verwenden die gleiche Firmware, die sich von derjenigen für die Telefentypen 2410 und 2420 unterscheidet.

Die folgende Tabelle beschreibt die Feldwerte, die von einem Administrator für den Firmware-Download hinzugefügt werden:

Bildschirm	Feld	Wert
Firmware-Station-Download	Download-Stationstyp	1408/1416
Status Firmware Station Download	Terminaltyp für Download	1408/1416
TFTP-Serverkonfiguration	Stationstyp	1408/1416

Hinweis:

Sie können die Firmware der Avaya 14xx Digitaltelefone mit den gleichen Methoden herunterladen, wie sie für die Avaya 24xx Digitaltelefone verwendet werden. Die 14xx Firmware ist ca. 40 % größer als die 24xx Firmware, dadurch verlängert sich die Kopierzeit.

Hinweis:

Die Avaya 14xx Digitaltelefone werden wie die Avaya 24xx Digitaltelefone in einer gemischten Umgebung verwaltet, d. h. beide Telefentypen (14xx und 24xx) sind innerhalb Ihrer Nebenstellenbereiche. Da diese Nebenstellen für den geplanten Firmware-Download angegeben wurden, sehen Sie "ABORT 8" Fehler in Zusammenhang mit den Nebenstellen. Wenn Sie beispielsweise die 14xx Firmware in Communication Manager geladen haben, wird 24xx die Firmware beim Aliasing ablehnen und Communication Manager wird den "ABORT 8" Fehler melden. Die Fehler erwähnen, dass die Nebenstellen für die aktuelle Firmware, die in Communication Manager geladen wurde, nicht korrekt sind. Diese Fehler können Sie jedoch ignorieren.

Ab Communication Manager 6.0 und darüber werden die Avaya 14xx Digitaltelefone nativ unterstützt und Sie können "ABORT 8" Fehler vermeiden, wenn Sie die Nebenstellen korrekt entweder als 1408 oder 1416 Telefentyp verwalten.

Rauschsignalunterstützung

RFC 3389 Rauschsignal

Wird angezeigt auf dem Bildschirm Signaling Group (Signalisierungsgruppe) wenn das Feld **Group Type** sip ist.

Gültige Einträge	Verwendung
y	Ermöglicht SIP-Signalisierung für Rauschsignal. Wenn das Feld RFC 3389 Comfort Noise (RFC 3389 Rauschsignal) auf y gestellt ist, setzt dieses Feld das Feld Silence Suppression (Signalaufrechterhaltung) auf dem Bildschirm IP Codec Set außer Kraft.
n	Deaktiviert SIP-Signalisierung für Rauschsignal. Vorgabe ist n.

Communication Manager Aktualisierungs- und Migrationspfade

Server-Migrationspfad für Communication Manager Version 5.2.1

In der folgenden Tabelle, gibt ✓ einen Migrationspfad an, der mit Kalkulation, Dokumentation und Konfigurationstool-Support unterstützt wird. ✗ an, dass es keinen unterstützten Migrationspfad gibt, aber die Wiederverwendung der Baugruppe und manuelle Konfiguration kann unterstützt werden.

Die für die Version 5.2.1 von Communication Manager unterstützten Migrationspfade sind in der folgenden Tabelle enthalten:

An → Von ↓	S8300 C/D	S8400 B	S8510	S8800 Simp- lex	S8730/S8800		
					Duplex	Hoch	Kri- tisch
CSI w/ CMC (An- mer- kung 1)	x	✓	✓	✓ (An- mer- kung 2)	✓ (Anmer- kung 2)	✓ (An- mer- kung 2,4)	x
S8100 w/CMC (An- mer- kung 2)	x	✓	✓	✓ (An- mer- kung 2)	✓ (Anmer- kung 2)	x	x
S8100 w/G600 (An- mer- kung 1)	x	✓	✓	✓ (An- mer- kung 2)	✓ (Anmer- kung 2)	x	x
SI Simp- lex	x	x	✓ (Anmer- kung 3, 4)	✓ (An- mer- kung 4)	✓ (Anmer- kung 4)	✓ (An- mer- kung 4)	✓ (Anmer- kung 4)
SI Dup- lex	x	x	x	x	✓ (Anmer- kung 4)	✓ (An- mer- kung 4)	✓ (Anmer- kung 4)
R Simp- lex/	x	x	x	✓	✓	✓	✓
R Dup- lex	x	x	x	x	✓	✓	✓
S8300 A/B/ C	✓	x	x	x	x	x	x
S8400 A	x	✓	✓	✓ (An- mer- kung 2)	✓ (Anmer- kung 2)	x	x
S8400 B	x	x	✓	✓	✓ (Anmer- kung 2)	x	x

An → Von ↓	S8300 C/D	S8400 B	S8510	S8800 Simp- lex	S8730/S8800		
					Duplex	Hoch	Kri- tisch
				(An- mer- kung 2)			
S8500 A/B/ C	x	x	✓	✓	✓	✓ (An- mer- kung 4)	✓ (Anmer- kung 4)
S8510	x	x	x	✓	✓	✓ (An- mer- kung 4)	✓ (Anmer- kung 4)
S8700 (IPC/ MC)	x	x	x	x	✓	✓	✓
S8710 (IPC/ MC)	x	x	x	x	✓	✓	✓
S8720 (IPC/ MC)	x	x	x	x	✓	✓	✓
S8730 (IPC/ MC)	x	x	x	x	✓ (Anmer- kung 5)	✓ (An- mer- kung 5)	✓ (Anmer- kung 5)

 Hinweis:

1. Gehäuse unterstützt keine duplizierten IPSIs
2. Nur Merges (System wird zu Port-Network in einem größeren System)
3. Nur Direktverbindung
4. Verwendung von G650 ist zwingend (Baugruppen aus einem anderen Gehäusetypp verschieben)
5. Migration zu S8800

Legende:

✓ - Migrationspfad wird unterstützt, Kalkulation, Dokumentation und Konfigurationstool-Support

✗ - Migrationspfad wird nicht unterstützt (dadurch wird die Baugruppenwiederverwendung und die manuelle Konfiguration nicht ausgeschlossen)

Bei Aktualisierungen unterstützte Server (nach Version)

Liste der in Version 5.2.1 von Communication Manager unterstützten Server:

Server	Communication Manager										
	1.x	2.0. ✗	2.1. ✗	2.2. ✗	3.0. ✗	3.1. ✗	4.0. ✗	5.0. ✗	5.1. ✗	5.2	5.2. 1
S8700	✓	✓	✓	✓	✓	✓	✓ *	✗	✗	✗	✗
S8710	✗	✗	✗	✓	✓	✓	✓	✓ +	✓ +	✓ +	✓ +
S8720	✗	✗	✗	✗	✗	✓	✓ ^	✓ ^+	✓ ^+	✓ ^+	✓ ^+
S8730	✗	✗	✗	✗	✗	✗	✗	✓ +	✓ +	✓ +	✓ +
S8800-S	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
S8800-D	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
S8500A	✗	✓	✓	✓	✓	✓	✓ *	✗	✗	✗	✗
S8500B	✗	✗	✗	✓	✓	✓	✓ *	✓ *	✓ *	✓ *	✓ *
S8500C	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓
S8510	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓
S8400A	✗	✗	✗	✗	✗	✓	✓	✓	✓ *	✓ *	✓ *
S8400B	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓

Ser- ver	Communication Manager										
	1.x	2.0. x	2.1. x	2.2. x	3.0. x	3.1. x	4.0. x	5.0. x	5.1. x	5.2	5.2. 1
S83 00A	✓	✓	x	x	x	x	x	x	x	x	x
S83 00B	x	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
S83 00C	x	x	x	x	x	x	✓	✓	✓	✓	✓
S83 00D	x	x	x	x	x	x	x	x	x	x	✓
S81 00	✓	✓	x	x	x	x	x	x	x	x	x
CSI	✓	✓	✓	✓	✓	✓	x	x	x	x	x
SI	✓	✓	✓	✓	x	x	x	x	x	x	x
R	✓	x	x	x	x	x	x	x	x	x	x

**Hinweis:**

- * unterstützt mit Speicheraktualisierung
- + erfordert DAL2 für Hardware-Dopplung
- ^ XL-Konfiguration erfordert DAL2 mit Hardware 1 Dopplung

Kernel-Austausch

Info über Kernel-Ersatz

Sie können den Linux-Kernel mit dem vorhandenen Update-Mechanismus in Communication Manager-Servern ersetzen, einschließlich Servern, die RAM-Disc unterstützen. Sie finden Informationen über Prozeduren zum Ersetzen des Kernel unter

- Kernel-Ersatz mit Communication Manager-System Management Interface
- Kernel-Ersatz mit Linux-Befehlen

Auch „Avaya Aura™ SIP Enablement Services release 5.2.1“ und „Avaya Software Update Manager (SUM)“ unterstützen Kernel-Aktualisierungen. Weitere Informationen zum Aus-

tausch des Kernel mit SUM, finden Sie unter *Avaya Integrated Management Release 5.2 Software Update Manager*.

Eine Kernel-Aktualisierung hängt nicht von Folgendem ab:

- Service-Pack, Sicherheits-Service-Pack oder SIP Enablement Services-Aktualisierungen
- Ob das System mit dem Kernel der Version läuft oder mit einem aus einem früheren Update



Hinweis:

Jede Aktualisierung der neuen Auslastung ist gesperrt, wenn eine Kernel-Aktualisierung aussteht.

Kernel-Austausch mit System Management Interface

Anmeldung bei System Management Interface (SMI) über das Laptop

-
1. Schießen Sie den Laptop mit einem Kreuzkabel an den Serviceport (eth1) an.
 2. Öffnen Sie Internet Explorer (5.5 oder darüber) auf dem Laptop.
 3. Im Feld **Address (or Location)** Ihres Browsers geben Sie **192.11.13.6** ein und drücken **Enter**.
Wenn Ihr Browser kein gültiges Sicherheitszertifikat hat, sehen Sie einen Warnbildschirm und Anweisungen, das Sicherheitszertifikat zu laden. Das System zeigt den Bildschirm Willkommen an.
 4. Klicken Sie auf **Continue**.
 5. Akzeptieren Sie die Client-Authentifizierung und das Sicherheitszertifikat.
Das System zeigt den Anmeldebildschirm an.
 6. Melden Sie sich als `craft` an.
 7. Wählen Sie **yes** für Suppress Alarm Origination (Alarmerzeugung unterdrücken).
Das System zeigt das Hauptmenü für SMI an.
 8. Klicken Sie im Menü **Administration** auf **Server (Maintenance)**.
Das System zeigt im linken Fenster das Hauptmenü an und eine Verwendungsvereinbarung im rechten Fenster.
-

Herunterladen der Kernel-Datei

Herunterladen der aktuellsten Kernel-Datei `.tar` von der Webseite <http://support.avaya.com>. Die Kernel-Datei kann aussehen wie folgt: `KERNEL-1.2.34-56.AB04XYZ.tar.gz`.



Hinweis:

Eine Product Correction Notice (PCN, Produktkorrekturhinweis)) wird ausgegeben, wenn ein neues Kernel-Update verfügbar ist. Wenn Sie die PCN sehen möchten, gehen Sie auf <http://support.avaya.com>.

Kopieren von Dateien auf den Server

1. Wählen Sie in der SMI **Miscellaneous > Download Files** (Verschiedenes > Dateien herunterladen).
Das System zeigt die Seite „Dateien herunterladen“ an.
2. Wählen Sie **File(s) to download from the machine I'm using to connect to the server**. (Datei(n) zum Herunterladen von der Maschine, um den Server zu verbinden)
3. Klicken Sie auf **Browse** (Durchsuchen), um das Fenster Choose File (Datei wählen) zu öffnen, und zu den Dateien zu navigieren, die Sie herunterladen möchten.
4. Wählen Sie die Dateien für den Download aus.
5. Klicken Sie auf **Download**, um die Dateien auf den Server zu kopieren.
Die Kernel-Datei wird in das Verzeichnis `/var/home/ftp/pub` kopiert.



Hinweis:

Wenn Sie manuell Dateien via FTP von Ihrem Laptop in das Verzeichnis `/var/home/ftp/pub` kopieren möchten, müssen Sie das Verzeichnis in `pub` (geben Sie ein `cd pub`) ändern, wenn Sie FTP gestartet und sich angemeldet haben.

Der Transfer ist abgeschlossen, wenn das System meldet: „Files have been successfully downloaded to the server“ (Die Dateien wurden erfolgreich auf den Server kopiert).

Installation der Kernel-Aktualisierung



Wichtig:

Sichern Sie die Serverdaten, bevor Sie den Kernel aktualisieren.

-
1. Wählen Sie in der SMI **Server Upgrades > Manage Updates** (Server-Upgrade > Updates verwalten).
Das System zeigt die Seite Manage Updates (Updates verwalten) an. Weitere Informationen hierzu finden Sie unter [Verwalten von Aktualisierungen](#) auf Seite 17.
 2. Wenn der Status der zu aktualisierenden Kernel-Aktualisierungsdatei `packed` in der Spalte `Status` anzeigt, wählen Sie die Datei (Radioschaltfläche) aus und klicken auf **Unpack** (Entpacken).
Das System zeigt den Status des Entpackens an.
 3. Klicken Sie wenn das System die Meldung "`...unpacked successfully`" anzeigt, auf **Continue** (Weiter).
Das System zeigt die Seite Manage Updates (Updates verwalten) an.
 4. Wenn das zu aktivierende Update `unpacked` in der Spalte `Status` anzeigt, wählen Sie die Datei (Radioschaltfläche) aus und klicken auf **Aktiviere** (Aktivieren).
Das System zeigt den Status des Aktivierungsprozesses an, und der Server startet automatisch neu. Der Serverneustart dauert ca. 3 bis 8 Minuten. Wenn der Server neugestartet wurde, läuft der alte Kernel.



Tipp:

Geben Sie, wenn Sie auf den Neustart des Systems warten `ping -t 192.11.13.6` von einer Eingabeaufforderung auf dem Service-Laptop ein, um einen kontinuierlichen Ping-Befehl zu starten. Wenn Sie eine Antwort erhalten, ist der Neustart abgeschlossen.

5. Prüfen Sie, ob das System korrekt läuft. Weitere Informationen hierzu finden Sie unter [Testen des Systems über die Systemmanagement-Schnittstelle](#) auf Seite 17.
 6. Kehren Sie zur Seite Manage Updates zurück.
 7. Wenn das zu aktivierende Update `Pending_Commit` in der Spalte `Status` anzeigt, wählen Sie die Datei (Radioschaltfläche) aus und klicken auf **Commit**.
-

Testen des Systems über die Systemmanagement-Schnittstelle

1. Klicken Sie auf der SMI auf **Administration > Server (Maintenance)** (Verwaltung > Server (Wartung)).
2. Klicken Sie unter **Server** auf **Status Summary** (Statusüberblick). Überprüfen Sie, ob die Felder `Server Hardware` und `Prozesse` „okay“ melden.
3. Wählen Sie unter **Diagnostics** (Diagnose) **Ping**.
4. Wählen Sie unter „Endpoints to Ping“ (Endpunkte für Ping) **All IPSI's, UPS's**.
5. Klicken Sie auf **Execute Ping** (Ping ausführen).
Ist Ping erfolgreich, zeigt die Seite Execute Ping results (Ping-Ergebnisse ausführen) eine kurze Zusammenfassung, die die Anzahl der gesendeten und empfangenen Pakete angibt. Die Zusammenfassung zeigt auch die Mindest-, Durchschnitts- und Höchstumlaufzeit an.
6. Verwenden Sie von einem Computer im Kunden-LAN den Internet Explorer, um eine Verbindung zum Server herzustellen..
7. Melden Sie sich mit **craft** an.
Mit dieser Aktion wird bestätigt, dass die Verbindung vorhanden ist, und der Kunde kann sich anmelden, um Verwaltungs- oder andere Aufgaben durchzuführen.

Verwalten von Aktualisierungen

Verwenden Sie diese Seite zur Verwaltung der Aktualisierungen. Die Aktualisierungsarten sind: Servicepack, Sicherheitsservicepack, Kernel und SIP Enablement Services-Aktualisierungen. Diese Seite zeigt an:

- Die aktuelle Version, die auf dem Server läuft
- Servermodus
- Verfügbare Aktualisierungen für den Server und ihren entsprechenden Status

Manage updates (Verwalten von Aktualisierungen) Felddescriptions

Name	Beschreibung
Update-ID	Die eindeutige Update-Kennung. Beispielsweise kann die Update-ID aussehen wie die folgende, für eine Kernel-Aktualisierung: <code>KERNEL-2.6.18-53.AB04XYZ</code> .
Status	Zeigt den Status der aktuellen Aktualisierung an.

Name	Beschreibung
	• Activated: Das Update funktioniert korrekt. • Packed: Ein neues Update ist verfügbar. • Unpacked: Ein neues Update wurde erfolgreich entpackt. • Pending_Commit: Das Kernel-Update wurde aktiviert aber die Aktivierung ist noch nicht zugewiesen. • Pending_Deactivate: Das Kernel-Update wurde deaktiviert aber die Deaktivierung ist noch nicht zugewiesen.
Typ	Entweder Heiß oder Kalt, wobei Kalt bedeutet, dass Update beeinflusst den Service, Heiß bedeutet, es hat keinen Einfluss auf den Service. Diese Seite fordert den Benutzer auf, fortzufahren, wenn das Update vom Typ Cold (Kalt) ist.
Unpack (Entpacken)	Entpackt die Aktualisierungsdatei. Die Aktualisierungsdatei wird im Aktualisierungs-Repository (<code>/var/home/ftp/pub</code>) gelesen.
View (Anzeigen)	Zeigt Informationen über die Aktualisierungsdatei an.
Activate (Aktivieren)	Aktiviert die Aktualisierungsdatei.
Deactivate (Deaktivieren)	Deaktiviert die Aktualisierungsdatei.
Remove (Löschen):	Entfernt alle zu einer Aktualisierungsdatei gehörenden Dateien, die nicht aktiv sind. Wenn das Update den Status <i>unpacked</i> hat und im Update-Repository liegt, wird das <i>Update</i> als <i>packed</i> angezeigt nachdem die Version <i>unpacked</i> gelöscht wurde.
Commit (Zuweisen)	Schließt den aktuellen Kernel-Aktualisierungsprozess ab. Das System zeigt den Status der aktuellen Kernel-Aktualisierung an.  Hinweis: Die Schaltfläche Commit ist nicht verfügbar, wenn die Kernel-Aktualisierung nicht den Status ausstehend hat.

Kernel-Austausch mit Linux-Befehlen

Verbindung eines Laptops mit dem Server

Voraussetzungen

Vergewissern Sie sich, dass Sie eine Secure Shell-(SSH)-Anwendung auf dem Laptop installiert haben, wie PuTTY.

-
1. Schließen Sie den Laptop mit einem Kreuzkabel an den Serviceport (eth1) an.
Wenn Sie kein Kreuzkabel haben, verwenden Sie ein IP-Hub.
Das System weist standardmäßig die IP-Adresse 192.11.13.6 an eth1 zu. eth1 ist die zweite Schnittstelle auf dem Server.
 2. Starten Sie eine SSH-Session.
 3. Geben Sie im Feld Host Name (oder IP-Adresse) Folgendes ein: 192.11.13.6.
 4. Klicken Sie im Bereich Protokoll auf **SSH**.
 5. Im Feld Port geben Sie Folgendes ein: 10022.
 6. Klicken Sie auf **Open**.



Hinweis:

Wenn Sie PuTTY verwenden, zeigt das System beim ersten Verbinden mit dem Server das Fenster PuTTY Security Alert an.

7. Klicken Sie auf **Yes**, um den Host-Key des Servers zu akzeptieren und das Fenster PuTTY anzuzeigen.
 8. Melden Sie sich als **craft** oder **dadmin** an.
 9. Geben Sie **Beenden** ein, und drücken Sie **Enter**, um PuTTY zu schließen.
-

Herunterladen der Kernel-Datei

Sie finden Anweisungen zum Herunterladen der Kernel-Dateien unter [Herunterladen der Kernel-Datei](#) auf Seite 15.

Kopieren von Dateien auf den Server

Sie finden Anweisungen zum Kopieren der Kernel-Dateien unter [Kopieren von Dateien auf den Server](#) auf Seite 15.

Installation der Kernel-Datei



Wichtig:

Sichern Sie die Serverdaten, bevor Sie den Kernel aktualisieren.

1. Geben Sie `update_unpack` ein, und drücken Sie **Enter**.
2. Wählen Sie die Datei aus, die der Kernel-Datei entspricht, und drücken sie **Enter**.
3. Geben Sie `update_show` ein, und drücken Sie **Enter**, um zu überprüfen, ob die neue Kernel-Datei entpackt wurde.
4. Geben Sie `update_activate kernel_name` ein, wobei `kernel_name` die Versions- oder Ausgabennummer der letzten Kernel-Datei ist.



Hinweis:

Verwenden Sie nicht die Erweiterung `.tar.gz` am Ende des Dateinamens.

5. Drücken Sie **Enter**. Das System zeigt die folgende Nachricht an, "WARNING: Activating this update will cause a server reboot. Continue?" (WARNUNG: Aktivierung diese Updates führt zum Server-Reboot. Fortfahren?)
6. Geben Sie `y` ein, und drücken Sie **Enter**.
Der Serverneustart dauert ca. 3 bis 8 Minuten. Wenn der Server neugestartet wurde, läuft der alte Kernel.



Tipp:

Geben Sie wenn Sie auf den Neustart des Systems warten `ping -t 192.11.13.6` von einer Eingabeaufforderung auf dem Service-Laptop ein, um einen kontinuierlichen Ping-Befehl zu starten. Wenn Sie eine Antwort erhalten, ist der Neustart abgeschlossen.

7. Melden Sie sich vom Service-Laptop mit einem SSH-Client beim Server an. Weitere Informationen hierzu finden Sie unter [Verbindung eines Laptops mit dem Server](#) auf Seite 19.
8. Prüfen Sie, ob das System korrekt läuft. Weitere Informationen finden Sie unter [Testen des Systems über die Systemmanagement-Schnittstelle](#) auf Seite 17.

9. Geben Sie `update_show` ein, und drücken Sie **Enter**, um zu überprüfen, dass der Status der Kernel-Datei `pending_commit` ist.
10. Geben Sie `update_commit` ein, und drücken Sie **Enter**.

**Hinweis:**

Wenn Sie nicht innerhalb von zehn Minuten nach dem Serverneustart den Befehl `update_commit` eingeben, wird geringfügiger Plattformalarm ausgelöst.

11. Geben Sie `update_show` ein, und drücken Sie **Enter**, um zu überprüfen, dass der Status der Kernel-Datei `Activated` ist.
-

Änderungen der bestehenden Befehle

`update_show`

Syntax

```
update_show [-a] [-c] [-h] [-k] [-u]
```

- a** Nur aktivierte Updates anzeigen.
- c** Anzeige der ausstehenden Updates sowie der Anzahl von Kernel-Updates.
- h** Anzeige der Befehlsoptionsbeschreibungen.
- k** Anzeige der Aktualisierungen vom Typ Kernel sowie der Anzahl der Kernel-Updates.
- u** Nur entpackte Updates anzeigen.

Beschreibung

Verwenden Sie `update_show`, wenn Sie Informationen über eine angegebene Software oder ein Kernel-Update wünschen.

`update_activate`

Syntax

```
update_activate [-h]
```

- h** Hilfe anzeigen.

Beschreibung

Verwenden Sie `update_activate`, um ein bislang nicht entpacktes Update auf dem Server zu aktivieren. Updates können nicht aktiviert werden, wenn ein Kernel-Update aussteht.

update_deactivate

Syntax

```
update_deactivate [-h]
```

-h Hilfe anzeigen.

Beschreibung

Verwenden Sie `update_deactivate`, wenn Sie ein zuvor aktiviertes Update auf dem Server deaktivieren möchten. Updates können nicht deaktiviert werden, wenn ein Kernel-Update aussteht.

Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer

Detaillierte Beschreibung von Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer

Verwenden Sie die Funktion Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer, um die Ruftonklassifizierungszeit und -genauigkeit zu verbessern, die für Stimm- und Anrufbeantworter-Anrufklassifizierung verwendet wird.

Diese Funktion liefert zwei Klassifizierungsmodi:

- ISDN beantworteter Anruf in AMD-AN-Modus – Erkennt Live-Stimme mit Anrufbeantworterererkennung (AMD).
- ISDN beantworteter Anruf in AMD-AUS-Modus – Erkennt Live-Stimme ohne AMD.

Diese beiden Modi erkennen keine Anruffortschrittkadenz außer Sonderhinweiston (SIT) und MODEM/FAX-Rückantwortton.

Diese Funktion verfügt auch über einen verwaltbaren Timer (End OCM timer), um sicher zu stellen, dass ein ausgehender Anruf, der OCM-Anrufklassifizierung nutzt, von einem Sachbearbeiter oder einer Ansage innerhalb einer bestimmten Zeit angenommen wird. Der Timer ist abgeschaltet, wenn der Anruf an einem Port angenommen oder beendet wird. Wenn der Timer abläuft, unterbricht Communication Manager den Anrufklassifikator und verbindet den Anruf mit einer Ansage.

Communication Manager lässt sich über das System verwalten, um den Klassifikator in einen der beiden Modi zu versetzen, je nachdem ob eine Verbindungs- oder Anrufüberwachungsmeldung von einer ausgehenden Amtsleitung erhalten wird.

 Hinweis:

Die Klassifikatorenmodi ohne Anruffortschrittskadenzerkennung müssen nicht mit dem End-OCM-Timer verwendet werden und umgekehrt. Die Klassifikatorenmodi mit Anruffortschrittserkennung können mit dem End-OCM-Timer verwendet werden.

Communication Manager verwaltet pro System, ob die Klassifikatoren die neuen Klassifizierungsmodi verwenden. Wenn Sie die Communication Manager-Software aktualisieren, verwenden die Klassifikatoren standardmäßig die alten Modi. Wenn Sie die Communication Manager-Software neu installieren, verwenden die Klassifikatoren standardmäßig die Nicht-Kadenz Anruftonklassifizierungsmodi.

Communication Manager verwaltet pro Standort die Höchstzeit nach der Antwort, die der Klassifikator mit dem Versuch verbringt, jeden OCM-Anruf zu klassifizieren. Der Timer reicht von 100 bis 25.000 Millisekunden in Schritten von 100 Millisekunden. Der Standard ist leer, was keine Einschränkung bedeutet.

Communication Manager verwaltet pro Standort eine Nebenstellenummer, um den Anruf zu verfolgen, wenn die maximale Klassifizierungszeit erreicht wurde. Die Nummer kann eine aufgezeichnete Ansage sein, eine Vektorverzeichnisnummer, eine Sammelgruppen-Nebenstellenummer oder leer. Das Feld **End of OCM intercept Extension** kann nicht leer bleiben, wenn das Timer-Feld **End OCM After Answer** einen nicht-leeren Wert enthält.

Firmware-Anforderungen für Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer

Für die TN744FP, TN2312AP/BP und TN8412AP Baugruppen sind die entsprechenden Firmware-Versionen 3, 48 und 18 oder darüber erforderlich, damit die Funktion unterstützt wird.

Für die G250, G350, G430, G450 und G700 Mediengateways, ist Firmware-Version-Load 30.10.x oder darüber erforderlich, damit die Funktion unterstützt wird.

Anrufbearbeitungsszenarien

Nachfolgend eine Liste der Anrufbearbeitungsszenarien für die Funktion Modi der Nicht-Kadenz-Anruftonklassifizierung und End-OCM-Timer:

ISDN-Amtsleitung

Bei der Verbindung eines Klassifizierers zu einem Anruf, weist Communication Manager den Klassifizierer an, die Modi der Nicht-Kadenz-Anruftonklassifizierung zu verwenden, wenn folgenden Bedingungen erfüllt sind:

- Der Anruf ist ein OCM-Switch-klassifizierter Anruf über eine ISDN-Amtsleitung.
- Ältere Versionen von Communication Manager verwenden die entsprechenden älteren Modi „AMD an“ oder „AMD aus“.

- Das Feld **Cadence Classification After Answer** (Kadenzklassifizierung nach Antwort) auf dem Bildschirm **System Parameters OCM Call Classification** (Systemparameter OCM-Ruftonklassifizierung) wurde auf N gesetzt.
- Communication Manager hat vom Ziel der Amtsleitung eine Connect-Nachricht erhalten und erfüllt eine der folgenden Bedingungen:
 - Das Feld **CONNECT Reliable When Call Leaves ISDN** im Bildschirm **ISDN Trunk Group** (ISDN-Amtsleistungsgruppe) steht auf Y.
 - Das Feld **CONNECT Reliable When Call Leaves ISDN** im Bildschirm **ISDN Trunk Group** (ISDN-Amtsleistungsgruppe) ist auf N gesetzt aber Communication Manager hat noch keine Meldung von der Fortschrittsanzeige erhalten, dass der Anruf nicht durchgehend ISDN ist oder der Anruf hat eine Zieladresse, die kein ISDN ist.

SIP-Amtsleitung

Bei der Verbindung eines Klassifizierers zu einem Anruf, weist Communication Manager den Klassifizierer an, die Modi der Nicht-Kadenz-Anrufklassifizierung zu verwenden, wenn folgende Bedingungen erfüllt sind:

- Der Anruf ist ein OCM-Switch-klassifizierter Anruf über eine SIP-Amtsleitung.
- Ältere Versionen von Communication Manager verwenden die entsprechenden älteren Modi „AMD an“ oder „AMD aus“.
- Das Feld **Cadence Classification After Answer** (Kadenzklassifizierung nach Antwort) auf dem Bildschirm **System Parameters OCM Call Classification** (Systemparameter OCM-Ruftonklassifizierung) wurde auf N gesetzt.
- Communication Manager hat ein Antwortsignal vom Ziel der Amtsleitung erhalten.

Andere Amtsleitungen (Nicht-ISDN & Nicht-SIP)

Bei der Verbindung eines Klassifizierers zu einem Anruf, weist Communication Manager den Klassifizierer an, die Modi der Nicht-Kadenz-Anrufklassifizierung zu verwenden, wenn folgende Bedingungen erfüllt sind:

- Der Anruf ist ein OCM-Switch-klassifizierter Anruf über eine Nicht-ISDN- oder Nicht-SIP-Amtsleitung.
- Ältere Versionen von Communication Manager verwenden die entsprechenden älteren Modi „AMD an“ oder „AMD aus“.
- Das Feld **Cadence Classification After Answer** (Kadenzklassifizierung nach Antwort) auf dem Bildschirm **System Parameters OCM Call Classification** (Systemparameter OCM-Ruftonklassifizierung) wurde auf N gesetzt.
- Das Feld **Answer Supervision Timeout** (Timeout der Antwortüberwachung) auf dem Bildschirm **Trunk Group** (Amtsleistungsgruppe) steht auf 0.
- Das Feld **Receive Answer Supervision** (Antwortüberwachung erhalten) auf dem Bildschirm **Trunk Group** (Amtsleistungsgruppe) steht auf y.
- Communication Manager hat ein Antwortsignal vom Ziel der Amtsleitung erhalten.

Mischung von alten und neuen Klassifizierern

Wenn ein IP-verbundenes Mediengateway oder Port-Network eine Mischung von neuen Klassifizierern aufweist, die die Nicht-Kadenz-Anrufklassifizierungsmodi verstehen und alten Klassifizierern, die diese Modi nicht verstehen, versucht die Anrufbearbeitung die neuen Klas-

sifizierer für OCM-Anrufe zu verwenden. Sind alle neuen Klassifizierer belegt, verwendet die Anrufweiterverarbeitung die alten Klassifizierer für OCM-Anrufe.

OCM-Timer beenden

- Wenn das Feld **End OCM After Answer** (OCM nach Antwort beenden) einen Wert enthält und nicht leer ist, startet Communication Manager den Timer für OCM-Anrufe nach Erhalt einer Connect-Nachricht oder einem Antwortüberwachungssignal vom Netzwerk.
- Wenn der End-OCM-Timer abläuft, verbindet Communication Manager anrufende Ende des Anrufs mit der Nebenstelle die im Feld **End of OCM Intercept Extension** (Ende der OCM Intercept-Nebenstelle) auf dem Bildschirm **Location Parameters** (Standortparameter) verwaltet wird.

Aktives VDN

Wenn die CTI-Anwendung eine dritte Partei auffordert, einen Anruf mit einer anrufenden VDN zu machen, richtet Communication Manager die anrufende VDN als aktive VDN ein. Wenn der End-OCM-Timer abläuft, leitet Communication Manager den Anruf an die Nebenstelle End-of-OCM Intercept weiter. Wenn Sie zulassen, dass das Feld **Allow VDN Override** (VDN übergehen zulassen) auf **n** gesetzt ist, beginnt die End-of-OCM Intercept-Nebenstelle, den Anruf zu verarbeiten, aber intern erinnert sich Communication Manager an den aktiven VDN als den anrufenden VDN.

Verwaltung von Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer

Folgende Schritte sind Teil der Verwaltung der Funktion Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer:

- Einrichten von Nicht-Kadenz Ruftonklassifizierungsmodi
- Einrichten von End-OCM-Timer-Nebenstelle

Der Abschnitt beschreibt:

- Die Bildschirme, die Sie verwenden, um die Funktion Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer zu verwalten
- Abschließen der Verwaltungsprozeduren für die Funktion Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer

Verwandte Themen:

[Einrichten von Nicht-Kadenz Ruftonklassifizierungsmodi](#) auf Seite 26

[Einrichten von End-OCM-Timer und der Ansagennebenstelle](#) auf Seite 26

Bildschirme für die Verwaltung von Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer

Bildname	Zweck	Felder
Systemparameter OCM-Ruftonklassifizierung	Richten Sie die Modi der Nicht-Kadenz-Ruftonklassifizierung ein.	Kadenzklassifizierung nach Antwort
Standortparameter	Richten Sie den Zeitintervall in Millisekunden für den End-OCM-Timer ein.	OCM nach Antwort beenden (ms)
	Richten Sie die Ankündigungserweiterung ein.	Ende OCM-Intercept-Erweiterung

Einrichten von Nicht-Kadenz Ruftonklassifizierungsmodi

-
1. Geben Sie `change system-parameters ocm-call-classification` ein. Drücken Sie `Enter`. Das System zeigt den Bildschirm "Feature-Related System Parameters" (Funktionsbezogene Systemparameter) an.
 2. Setzen Sie das Feld **Cadence Classification After Answer** (Kadenzklassifizierung nach Antwort) auf `n`.
 3. Drücken Sie `Enter`, um Ihre Änderungen zu speichern.
-

Einrichten von End-OCM-Timer und der Ansagennebenstelle

-
1. Typ `Standortparameter` ändern. Drücken Sie `Enter`. Das System zeigt den Bildschirm „System Parameters OCM Call Classification“ (Systemparameter OCM Anruftklassifizierung) an.
 2. Geben Sie im Feld **End OCM After Answer (ms)** den gewünschten Timeout-Wert in Millisekunden ein. Gültige Einträge sind eine Zahl von 100 bis 25.000 oder nichts. Im Feld **End of OCM Intercept Extension** geben Sie die Nebenstellenummer ein, die Sie zuordnen möchten. Die Nummer kann eine aufgezeichnete

Ansage, eine Vektorverzeichnisnummer oder eine Sammelgruppen-Nebenstellennummer sein.

3. Drücken Sie **Enter**, um Ihre Änderungen zu speichern.

Bedingungen für Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer

Dieser Abschnitt informiert darüber, wie sich die Funktion Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer unter bestimmten Bedingungen verhalten. Verwenden Sie diese Information, damit Sie unter allen Bedingungen maximalen Nutzen aus Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer ziehen können. Folgende Betrachtungen treffen für die Funktion Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer zu.

Ansagen

Zur Verhinderung von Verspätungen bei der Verbindung zur Ansage,

- können Sie Communication Manager mit einem großen Pool von Ansagebaugruppen konfigurieren.
- können Sie Communication Manager so konfigurieren, dass integrierte Wiederholungen der Ansagen verwendet werden. Dieser Ansagetyp lässt Anrufe den Ansagen-Port verwenden, auch wenn dieser bereits verwendet wird.

Für jede dieser Konfigurationen muss jedes Gateway mit öffentlichen Netzwerksamtsleitungen eigene Ansage-Ports haben, lokal für das Gateway zur Nutzung durch die Funktion Lokaler Ansagequellen.

Auswirkungen auf die Performance

Die Werte der Felder **AMD Treatment Talk Duration** (AMD-Treatment Gesprächsdauer) und **AMD Treatment Pause Duration** (AMD-Treatment Pausendauer) auf dem Bildschirm **SIT Treatment for Call Classification** (SIT-Treatment für Ruftonklassifizierung) können Einfluss auf die Klassifizierungszeit haben. Diese Funktion verringert die Ruftonklassifizierungshaltezeiten, erhöht aber die Verwendung der aufgezeichneten Ansagen.

Call Management System (CMS) und Avaya IQ

Sie können CMS verwalten, so dass ein Bericht über den Prozentsatz der Anrufe erstellt wird, die von einer Person entgegengenommen wurden, aber wegen Zeitüberschreitung vor der Verbindung mit einem Sachbearbeiter mit **End of OCM Intercept Extension** verbunden wurden.

AMD falsche Positive

Sie können die Ruftonklassifizierungs-Timer so verwalten, dass eine niedrige Rate von falsch positiven Anrufbeantwortern erkannt wird, dabei werden andere Einflüsse von außen nicht beachtet. Es ist jedoch eine gewisse Entdeckungsrate falsch positiver Anrufbeantworter zu erwarten, aufgrund von Faktoren wie Schwankungen in der Art, wie Personen Telefongespräche mit unterschiedlichen Begrüßungsformeln annehmen.

AMD für eine Nicht-AMD Callcenter

Callcenter können in ihren Berechnungen zulassen, Anrufe zu ignorieren, die am Ziel von Anrufbeantwortern entgegengenommen wurden. Sie können ein Nicht-AMD-Callcenter so

verwalten, dass Live-Stimmanrufe verfolgt werden, mit Ausnahme von Anrufbeantworteranrufen, und beweisen, dass weniger als der zulässige Prozentsatz von Stimmanrufen abgebrochen wurde, weil kein Sachbearbeiter verfügbar war.

Klingelvorschrift

Callcenter können zulassen, dass ausgehende Anrufe für eine bestimmte Zeit klingeln (die Klingelvorschrift variiert von Land zu Land), wenn Anrufe vom Angerufenen nicht entgegen genommen werden. Sie entsprechen der Vorschrift, wenn Sie Folgendes tun:

- Programmieren Sie die CTI-Anwendung so, dass sie die Felder „Option Dritte Person ruft an“ und **max_ring_cycles** verwendet.
- Weisen Sie die Sachbearbeiter im Callcenter an, Anrufe nicht zu trennen, bevor eine bestimmte Zeit vergangen ist, wenn ihr Anruf mit einem Klingeln verbunden wurde.

Unabhängige Benutzergruppen

Die Funktion Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer kann mit einem einzelnen Communication Manager-Server verwendet werden, der unter mehreren unabhängigen Benutzergruppen gemeinsam verwendet wird, jeder einzelne hat dabei seine eigene Ansage. Um mehrere unabhängige Benutzergruppen zu unterstützen, muss die CTI-Ergänzung den anrufenden VDN vorbestimmen, der mit „Third party make call“ zu verwenden ist, mindestens ein anrufender VDN pro unabhängiger Benutzergruppe. Sie können das Feld "End of OCM Intercept Extension" mit einem einzelnen VDN verwalten, der im Gegenzug den Anruf zu der richtigen Ansage für jede unabhängige Benutzergruppe weiterleitet.

Alternativ können Sie eine einzelne anrufende VDN-Nebenstelle verwenden, die unter mehreren Benutzergruppen gemeinsam benutzt wird, und den Anruf an CTI-Handling über einen ergänzenden Routing-Schritt zurücksenden. Die CTI-Anwendung kann den Anruf an eine Ansage weiterleiten, die dem anrufenden Benutzer entspricht. Diese alternative Strategie benötigt im Vergleich zu der VDN-Strategie mehr Zeit.

Interaktionen für Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer

Dieser Abschnitt informiert darüber, wie die Funktion Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer mit anderen Funktionen im System interagiert. Verwenden Sie diese Information, damit Sie in jeder Funktionskonfiguration maximalen Nutzen aus Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer ziehen können.

Multinationale/Globale Betrachtungen

Das Feld **Cadence Classification After Answer** (Kadenzklassifizierung nach Antwort) im Bildschirm **System Parameters OCM Call Classification** (Systemparameter OCM-Ruftonklassifizierung) wird eher nach System als nach Standort konfiguriert.

Das Timer-Feld **End OCM After Answer** (OCM nach Antwort beenden) wird nach Standort verwaltet. Es ist wahrscheinlich, dass verschiedene Länder unterschiedliche Zeitvorschriften haben.

Das Feld **End of OCM Intercept Extension** (Ende OCM-Intercept-Erweiterung) wird nach Standort verwaltet. Es ist wahrscheinlich, dass verschiedene Länder Ansagen in unterschiedlichen Sprachen haben.

TTY-Klassifizierung

Der Anrufklassifikator hat aktuell keine TTY-Erkennung. Sie können eine Ansage in der lokalen Sprache und in TTY aufzeichnen. Das Feld **End of OCM Intercept Extension** (Ende OCM-Intercept-Erweiterung) kann eine aufgezeichnete Ansage in der (den) lokalen Sprache(n) und in TTY enthalten.

Ruftonklassifizierung nach Antwortüberwachung

Die Funktion Ruftonklassifizierung nach Antwortüberwachung ist nicht abhängig von der Funktion Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer.

CONNECT reliable when call leaves ISDN

Die Funktion Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer hängt vom Feld **CONNECT reliable when call leaves ISDN** ab.

Antwortüberwachung Zeitüberschreitung:

Wenn die Antwortüberwachung aktiviert ist, setzen Sie das Feld **Answer Supervision Timeout** (Antwortüberwachung Zeitüberschreitung) auf 0 (Null).

Private Network ISDN (QSIG)

Communication Manager sendet eine Aktualisierungsnachricht an die QSIG-Amtsleitung, wenn Folgendes passiert:

- Die abgehende Amtsleitung verwendet „QSIG Private Networking Signaling“.
- Communication Manager ändert den Anrufer vom in der Anforderung „CTI-Zusatz Third Party Make Call“ angegebenen in End of OCM Intercept Extension (Ende OCM-Intercept-Erweiterung).

Es handelt sich um die gleiche Nachricht, die verwendet wird, wenn eine Person den Anruf manuell weiterverbindet. Es ist jedoch nicht wahrscheinlich, dass in einem Callcenter abgehende Anrufe über QSIG-Amtsleitungen erfolgen.

SIP

Communication Manager sendet eine Aktualisierungsnachricht an die SIP-Amtsleitung, wenn Folgendes geschieht:

- Die abgehende Amtsleitung verwendet SIP-Signalisierung.
- Communication Manager ändert den Anrufer vom in der Anforderung „CTI-Zusatz Third Party Make Call“ angegebenen in End of OCM Intercept Extension (Ende OCM-Intercept-Erweiterung).

CCRON

Communication Manager teilt die Nicht-Kadenz Rufunklassifizierungsmodi nicht mit der Funktion „Weiterleitung von netzextern umgeleiteten Anrufen“ (Coverage of Calls Redirected Off-Net - CCRON).

EC500

Communication Manager teilt die Nicht-Kadenz Rufunklassifizierungsmodi nicht mit der Funktion „Nebenstelle zu Mobiltelefon“ (Extension to Cellular - EC500).

Verbindungssteuerung über Vektoren

Verbindungssteuerung über Vektoren funktioniert mit der Funktion Nicht-Kadenz Rufunklassifizierungsmodi und End-OCM-Timer .

Alternative Inter-Gateway-Leitweglenkung

Wenn Sie eine einzelne PBX für die Callcenter- und Nicht-Callcenter-Kommunikation haben, kann ein Callcenter mit strikter Zeitregulierung „Alternative Inter-Gateway-Leitweglenkung“ (Inter-Gateway Alternate Routing - IGAR) verwenden. Sie müssen sicherstellen, dass jedes Gateway mit öffentlichen Netzwerkamtsleitungen über (einen) eigene(n) Ansagen-Port(s) zur Nutzung für die Lokalen Ansagen verfügt. Auf diese Weise werden Verzögerungen bei der Verbindung mit den Ansagen vermieden.

Rufumleitung

Communication Manager 5.2.1 behandelt einen OCM-Anruf genauso wie die Communication Manager 5.0 „Third Party Make Call“-Funktion, wenn Folgendes passiert:

- Communication Manager beendet einen OCM-Anruf an die Nebenstelle „End of OCM Intercept“.
- Die „Nebenstelle End of OCM Intercept“ wird als VDN verwaltet.
- Der zugeordnete Vektor verfügt über einen Route-to-Schritt.

Der Anruf wird zum nächsten Route-to-Ziel weitergeleitet. Wenn der Anruf an einem besetzten Endpunkt endet, unterbricht Communication Manager den Anruf.

Einheitlicher Rufnummernplan

Communication Manager verwaltet pro Standort eine Nebenstellenummer, um den Anruf zu verfolgen, wenn die maximale Klassifizierungszeit erreicht wurde. Die Nebenstellenummer kann eine aufgezeichnete Ansage, eine VDN oder eine Nebenstellenummer einer Sammel-

gruppe auf dem lokalen Server sein. Das Feld akzeptiert keine UDP-Nebenstelle, auch nicht, wenn die Nebenstelle an eine aufgezeichnete Ansage auf einem anderen Server weiterleitet.

ARS-Routing an mehreren Standorten

Der Standort der abgehenden Amtsleitung wird für den OCM-Anruf verwendet, wenn Folgendes geschieht:

- Communication Manager beendet einen OCM-Anruf an die Nebenstelle „End of OCM Intercept“.
- **End of OCM Intercept Extension**, die „Nebenstelle End of OCM Intercept“, wird als VDN verwaltet..
- Der zugeordnete Vektor verfügt über einen Route-to-Schritt.

„Rufnummernplan für mehrere Standorte“ (Multi-Location Dial Plan - MLDP)

Die Funktion „Rufnummernplan für mehrere Standorte“ analysiert Ziffernfolgen anhand von Einträgen in die UDP-Tabellen. **End of OCM Intercept Extension** kann nicht wie eine UDP-Nebenstelle verwaltet werden. Sie können die vollständige Nebenstellenummer in das Administrationsfeld eingeben.

Standortparameter

Beenden von OCM nach Antwort (ms)

Wenn das Feld **End OCM After Answer** einen nicht-leeren Wert enthält, startet Communication Manager den End-OCM-Timer, wenn Communication Manager ein Antwortsignal erhält. Der End-OCM-Timer stellt sicher, dass ein abgehender Anruf, der OCM Ruftonklassifizierung verwendet, innerhalb einer angegebenen Zeit von einem Sachbearbeiter wird oder einer Ansage angenommen wird.

Gültiger Eintrag	Verwendung
100 bis 25.000	Der Zeitüberschreitungswert wird in Millisekunden angegeben. Wenn der Timer abläuft, unterbricht Communication Manager den Anrufklassifikator und verbindet den Anruf mit der verwalteten Intercept-Nebenstelle. Wenn der Ruftonklassifizierer den Anruf klassifiziert, bevor der Timer abläuft, wird der Timer abgebrochen und der Anruf weitergeleitet und korrekt behandelt.

Gültiger Eintrag	Verwendung
Leer	Zeigt an, dass der Timer keine Begrenzung hat.

Ende OCM-Intercept-Erweiterung

Gültiger Eintrag	Verwendung
Nebenstelle	Die Nebenstellenummer Communication Manager verbindet den Anruf, wenn das Feld End OCM After Answer abläuft. Die Nebenstellenummer kann eine aufgezeichnete Ansage, eine Vektorverzeichnisnummer oder eine Sammelgruppen-Nebenstellenummer.
Leer	Gibt an, dass die Nebenstellenummer leer ist. Wenn das Feld End OCM After Answer auf einen nicht-Leeren Wert gesetzt wurde, kann das Feld End of OCM Intercept Extension nicht leer bleiben.

Systemparameter OCM-Ruftonklassifizierung

Kadenzklassifizierung nach Antwort

Gültiger Eintrag	Verwendung
y	Alter Klassifizierer ermittelt Live-Stimme mit oder ohne AMD. Diese Modi erkennen Hörtonkadenzen. Wenn Sie die Communication Manager Software aktualisieren, verwendet der Klassifizierer standardmäßig die alten Modi. Wenn Sie die Communication Manager Software neu installieren, verwendet der Klassifizierer standardmäßig die Nicht-Kadenz Klassifizierungsmodi.
n	Nicht-Kadenz Klassifizierungsmodi erkennen Live-Stimme mit oder ohne AMD, wenn Communication Manager eine Verbindungs- oder Anwortsüberwachungsmeldung von einer ausgehenden Amtsleitung erhält. Diese Modi erkennen keine Hörton-Kadenz.

Connection Manager Ablehnungsereignisse

DNY_CLASS_NO_CAP

Tabelle 1: Connection Manager Ablehnungsereignisse

Ereignis- typ:	Ereignisbe- schreibung, wie sie im Ereignispro- tokoll ange- zeigt wird	Erklärung	Ereignis- daten 1	Ereignis- daten 2
2399	DNY_CLASS_NO_CAP	CPTR angefordert mit Nicht-Kadenzeigen- schaften, nicht gefun- den.		

Spezialanwendung, Aktivierungsprozess

Spezialanwendungen, auch bekannt als grüne Funktionen, erfüllen bestimmte Anforderungen, die von ein oder mehreren Kunden beantragt worden sind. Bislang hat Avaya dem Kunden für die Aktivierung der Spezialanwendungen eine Gebühr berechnet. Communication Manager bietet jetzt viele der Spezialanwendungen allen Kunden ohne zusätzliche Kosten oder Änderungen der Lizenz an. Kunden können die Spezialanwendungen selbst über das eigene Super-User-Login aktivieren. Obwohl diese Spezialfunktionen den Kunden zur Verfügung stehen, sind sie möglicherweise nicht so ausführlich getestet worden. Kunden verwenden sie also auf eigenes Risiko.

Einige der Spezialfunktionen sollten nicht ohne die richtige Konfiguration eingerichtet werden, und andere Funktionen sollten nicht gleichzeitig verwendet werden. Andernfalls reagiert die Funktion nicht wie erwartet, die System-Performance könnte beeinträchtigt werden, oder beides. Damit Benutzer diese Funktionen nicht aus Versehen einrichten, hat Communication Manager diese Funktionen gekennzeichnet und als eingeschränkt markiert. Für das Aktivieren dieser beschränkten Funktionen müssen Kunden Kontakt mit Avayas Custom Development Team aufnehmen.

Eine Liste der uneingeschränkten Spezialfunktionen und Informationen darüber finden Sie unter *Avaya Aura™ Communication Manager Special Application Features*, verfügbar unter <http://support.avaya.com>.

Kapitel 2: Avaya-Mediengateways, Änderungen

In diesem Kapitel werden die Änderungen der Funktionen in den Mediengateways für Avaya Aura™ Communication Manager 5.2.1 zusammengefasst

G450 - erhöhte Kapazität

Das G450 unterstützt jetzt insgesamt 320 VoIP-Kanäle.



Hinweis:

Die erhöhte Kapazität ist nur verfügbar, wenn das G450 mit einem Server registriert ist, auf dem Communication Manager 5.2.1 oder höher läuft.

Die Ausgabe des CLI-Befehls `show voip-parameters` reflektiert den neuen Wert:

show voip-parameters

Syntax

```
show voip-parameters
```

Beschreibung

Verwenden Sie den Befehl `show voip-parameters`, um Informationen über die VoIP-Engine anzuzeigen.

Benutzer-Level

Nur-Lesen

Kontext

allgemein

Beispiel

Um VoIP-Information anzuzeigen:

```
G450-001(super)# show voip-parameters
VOIP ENGINE PARAMETERS
-----
IP (PMI)                : 149.49.71.15
Fault Status            : No Fault Messages
```

Additional Status : No Status Messages

CURRENT STATE

In Use : 0 of 320 channels, 0 of 9600 points (0.0% used)
...

MP20 - erhöhte Kapazität

G430 und G450 unterstützen jetzt 25 VoIP-Kanäle auf dem MP20-Medienprozessormodul.



Hinweis:

Die erhöhte Kapazität ist nur verfügbar, wenn G430 oder G450 mit einem Server registriert ist, auf dem Communication Manager 5.2.1 oder höher läuft.

Die Ausgangspegel der folgenden CLI-Befehle spiegeln den neuen Wert wieder:

- `show voip-parameters`
- `show voip-dsp`
- `show system`
- `show platform mainboard`

Avaya G430 CLI-Befehle

show voip-dsp

Syntax

`show voip-dsp [dsp-id]`

dsp-id Schlüsselwort, dass Steckplatznummer der VoIP DSP-Unterplatine angibt.

dsp-id Mögliche Werte:

- 1 - DSP auf der Hauptplatine
- 2 - austauschbares DSP

Beschreibung

Verwenden Sie den Befehl `show voip-dsp`, um Informationen über Parameter, Status und Auslastung der DSP- und DSP-Cores anzuzeigen.

Benutzer-Level

Schreibgeschützt

Kontext

allgemein

Beispiel

Zur Anzeige von DSP-Parametern:

```
G430-???(super)# show voip-dsp

DSP #1 PARAMETERS
-----
Board type       : 25 Channels on board VoIP DSP
Fw Vintage       : 16

DSP#1 CURRENT STATE
-----
In Use           : 0 of 25 channels, 0 of 750 points (0.0% used)
State            : Idle
Admin State      : Release
```

show voip-parameters

Syntax

```
show voip-parameters
```

Beschreibung

Verwenden Sie den Befehl `show voip-parameters`, um Informationen über die VoIP-Maschine anzuzeigen.

Benutzer-Level

Schreibgeschützt

Kontext

allgemein

Beispiel

um VoIP-Information anzuzeigen:

```
G430-003(super)# show voip-parameters
```

VOIP ENGINE PARAMETERS

```
-----
IP (PMI)           : 149.49.71.15
Fault Status       : No Fault Messages
Additional Status   : No Status Messages
```

CURRENT STATE

```
-----
In Use           : 0 of 105 channels, 0 of 3150 points (0.0% used)
```

VoIP-DSPs PARAMETERS

```
-----
VoIP Child Type SUFFIX HW      FW      Chan  Admin  Oper  Fault
Slot Board                VINTAGE VINTAGE InUse  State  State Status
-----
1      On board(25)      N/A      16      0/25 Release Idle  No Error
2      VOIP  MP80 B      0      16      0/80 Release Idle  No Error
...
```



Hinweis:

Wenn G430 für Versionen von Communication Manager vor 5.2.1 registriert ist, die die erhöhte Kapazität nicht unterstützen, wird folgende Meldung angezeigt:

Note: The gateway is registered with a Communication Manager version which limits DSP resources to 100 channels.

System anzeigen

Syntax

```
show system
```

Beschreibung

Verwenden Sie den Befehl `show system`, um Informationen über das Gerät anzuzeigen.

Benutzer-Level

Schreibgeschützt

Kontext

allgemein

Beispiel

Zur Anzeige von Geräteinformationen:

```
G430-??? (super)# show system
System Name      :
System Location   :
System Contact    :
Uptime (d,h:m:s) : 2,18:20:56
```

```

MV Time                : 09:39:53 26 MAR 2009
Serial No              : 08IS26191007
Model No               : G430
HW Ready for FIPS      : No
HW Vintage             : 4
HW Suffix              : F
FW Vintage             : 29.22.1
LAN MAC Address        : 00:07:3b:e4:67:b9
SERVICES MAC address   : 00:07:3b:e4:67:b8
RAM Memory             : 512MB
Compact Flash Memory   : CompactFlash card is disabled
Main PSU               : 175W
Media Socket #1        : 25 channels on board VoIP DSP
Media Socket #2        : MP20 VoIP DSP Module
FANS                   : No Fault messages
Expansion module #1    : OK
Expansion module #1 PSU : 175W
Expansion module #1 POE PSU : Not present
Expansion module #1 FANS : No Fault messages
Expansion module #2    : Not Present

```

show platform mainboard

Syntax

```
show platform mainboard
```

Beschreibung

Verwenden Sie den Befehl `show platform mainboard`, wenn Sie die Parameter der Hauptplatine und die Liste der in den Steckplätzen der Hauptplatine installierten Mediengateway-Ausrüstung anzeigen möchten.

Benutzer-Level

admin

Context

allgemein

Beispiel

Wenn Sie die Parameter der Hauptplatine und die Liste der Mediengateway-Ausrüstung anzeigen möchten:

```

G430-??? (super) # show platform mainboard
MAINBOARD BOARD
-----
Type                : G430
Description          : Avaya Inc., G430 Media Gateway
Serial Number       : 08IS26191007
HW Vintage          : 4
HW Suffix           : F
FW Version          : 29.22.1
Faults              : No Fault Messages

```

```
RAM MEMORY SOCKET #1
-----
Type                : 512MB DDR SDRAM memory module
Serial Number       : 0b2c7605
Manufacture Part Num : 64A6M64M8L-A06EWQU
Faults              : No Fault Messages

COMPACT FLASH MEMORY
-----
Type                : CompactFlash card is disabled
Serial Number       : N/A
Model Number        : N/A
Faults              : N/A

MEDIA SOCKET #1
-----
Type                : 25 channels on board VoIP DSP
Description         : VoIP DSP resource with 20 channels
Faults              : No Fault Messages

MEDIA SOCKET #2
-----
Type                : MP20 VoIP DSP Module
Description         : VoIP DSP resource with 25 channels
Serial Number       : 08IS18183392
HW Vintage          : 1
HW Suffix           : A
Faults              : No Fault Messages
```

Avaya G450 CLI-Befehle

show voip-dsp

Syntax

```
show voip-dsp [dsp-id]
```

dsp-id Schlagwort, dass Steckplatznummer der VoIP DSP-Unterplatine angibt.

dsp-id Mögliche Werte: 1 bis 4

Beschreibung

Verwenden Sie den Befehl `show voip-dsp`, um Informationen über Parameter, Status und Auslastung der DSP- und DSP-Cores anzuzeigen.

Benutzer-Level

Schreibgeschützt

Context

allgemein

Beispiel

zur Anzeige von DSP-Parametern:

```
G450-003(super)# show voip-dsp
DSP #1 PARAMETERS
-----
Board type       : MP20
Hw Vintage      : 2 A
Fw Vintage      : 16

DSP#1 CURRENT STATE
-----
In Use          : 0 of 25 channels, 0 of 750 points (0.0% used)
State           : Idle
Admin State     : Release

Core# Channels Admin      State
      In Use   State
-----
   1   0 of 25 Release Idle
....
```

show voip-parameters

Syntax

```
show voip-parameters
```

Beschreibung

Verwenden Sie den Befehl `show voip-parameters`, um Informationen über die VoIP-Maschine anzuzeigen.

Benutzer-Level

Schreibgeschützt

Kontext

allgemein

Beispiel

um VoIP-Information anzuzeigen:

```
G450-001(super)# show voip-parameters

VOIP ENGINE PARAMETERS
-----
IP (PMI)           : 149.49.70.159
Fault Status       : No Fault Messages
Additional Status   : No Status Messages

CURRENT STATE
-----
In Use             : 0 of 25 channels, 0 of 750 points (0.0% used)

VoIP-DSPs PARAMETERS
-----
VoIP Child Type SUFFIX HW      FW      Chan  Admin  Oper  Fault
Slot Board          VINTAGE VINTAGE InUse  State  State  Status
-----
-----
1    VOIP  MP20  A      2        16      0/25 Release Idle  No Error
2    -- Not Installed --
3    -- Not Installed --
4    -- Not Installed --
Done!
```

Hinweis:

Wenn G450 für Versionen von Communication Manager vor 5.2.1 registriert ist, die die erhöhte Kapazität nicht unterstützen, wird folgende Meldung angezeigt:

Note: The gateway is registered with a Communication Manager version which limits DSP resources to 240 channels.

ARP-Spoofing-Schutz

ARP-Spoofing-Schutz hält Angreifer davon ab, kostenlose ARPs auszunutzen, um DoS (Denial of Service) oder "Man-in-the-middle"-Attacken zu generieren.

Der ARP-Spoofing-Schutz funktioniert über das Erlernen der neuen ARP-Einträge aus den Unicast ARP-Antworten, die als Antworten an Gateway-ARP-Anforderungspakete versendet wurden.



Hinweis:

Der ARP-Spoofing-Schutz wird am Service-Port nicht unterstützt.

Der Benutzer aktiviert oder deaktiviert den ARP-Spoofing-Schutz mit dem CLI-Befehl „ip arp inspection“:

ip arp inspection

Syntax

```
[Nein] ip arp inspection
```

Beschreibung

Verwenden Sie den Befehl `ip arp inspection`, um den ARP-Spoofing-Schutz zu aktivieren oder zu deaktivieren.

Benutzer-Level

admin

Kontext

allgemein

Beispiel

Zur Aktivierung von ARP-Spoofing-Schutz:

```
G430-001(super)# ip arp inspection
```

Zur Deaktivierung von ARP-Spoofing-Schutz:

```
G430-001(super)# no ip arp inspection
```

Protokollerweiterungen

Die Mediengateways stimmen mit dem neuen Avaya-Standard für das allgemeine Protokollformat überein. Es handelt sich um das Format

```
< PRI > Date stamp hostname MSG
```

S2

Es wird definiert von RFC 3164. Es repräsentiert den Verbindungsweg und die Dringlichkeit der Nachricht.

Header

Der Header-Teil enthält einen Zeitstempel sowie die Anzeige des Hostnamens oder der IP-Adresse des Geräts.

MSG

Die Gateways unterstützen die zusätzlichen Felder als Teil des Abschnitts MSG im Syslog und der in der CLI-Session repräsentierten Log-Einträge, Ansicht der Log-Datei und der auf den Remote-Server hochgeladenen Log-Datei. Siehe „Zusätzliche Felder für MSG-Tabelle“.

Tabelle 2: Zusätzliche Felder für MSG

SI no	Punkt	Allgemeines Protokollformat SRAD-Beschreibung	Gateway-Feldwert
1	TAG [Prozess-ID]	TAG ist der Name der Anwendung.	Das Gateway zeigt an „-NoTAG:“.
2	UTC Offset	UTC Offset	Das Gateway zeigt nur an „-NoUTC:“.
3	Jahr	4-stelliges Jahr - wenn nicht unterstützt oder unbekannt, dann 0000.	Die Gateways zeigen das Jahr basierend auf MV-Zeit an, wenn das Gateway registriert ist; auf RTC-Zeit, wenn es nicht registriert ist (G430, G450 und die neuen G250/G350 C/S: 4.0/3.1 respektive und darüber).
4	Millisekunden	Millisekunden im 3-Stellenformat.	Millisekunden
5	Protokollformat	Wert „1“ steht für den aktuell definierten Protokollformat-Header	Das Gateway zeigt „1“ an

Sl no	Punkt	Allgemeines Protokollformat SRAD-Beschreibung	Gateway-Feldwert
6	Produkttyp	Der Produkttypname:	Die Gateways zeigen an: ".mediagateway.g450", ".mediagateway.g430", ".mediagateway.g350", ".mediagateway.g250", ".mediagateway.g250bri", ".mediagateway.g250ds1", ".mediagateway.g250dcp"
7	Kennzeichnung	Das Zeichen „ “ markiert den Anfang der Nachricht.	Das Gateway zeigt „ “ an
8	Nachrichtenformat	Wert 0 zur Darstellung von Nicht-Ereignisprotokollen. Wert 1 und 2 für Ereignisprotokolle.	Das Gateway unterstützt nur Wert „0“ für Nicht-Ereignisprotokolle.
9	Mnemonisch	Ein 32-Byte-String, der die Protokollnachricht kurz beschreibt.	
10	Kennzeichnung	Das Zeichen „[“ trennt zwischen der mnemonischen und Syslog-Filtergruppe/-dringlichkeit.	Das Gateway zeigt „[“ an
11	Syslog-Filtergruppe	Der Benutzer wählt die Gruppe mit dem Befehl CLI.	
12	Syslog-Dringlichkeit	Der Benutzer wählt die Dringlichkeit mit dem Befehl CLI.	

Beispiel

Beispiele für das neue Syslog/Log:

```
<190>Apr 21 16:28:32 149.49.77.11 -NoTag: -NoUTC 2009 055 1 mediagateway.g430 | 0 coldStart[BOOT-Informational: System boot up from cold reset, ID=N/A
<187>Apr 21 16:28:32 149.49.77.11 -NoTag: -NoUTC 2009 525 1 mediagateway.g430 | 0 MSY-TRMAJNA[VOICE-Error: No Call Controller Found, ID=N/A
<190>Apr 21 14:30:25 149.49.77.11 -NoTag: -NoUTC 2009 965 1 mediagateway.g430 | 0 BOOT MESSAGE[BOOT-Informational: Booting from bank B with firmware version 29.22.50, ID=N/A
<190>Apr 21 14:30:25 149.49.77.11 -NoTag: -NoUTC 2009 965 1 mediagateway.g430 | 0 coldStart[BOOT-Informational: System boot up from
```

```
cold reset, ID=N/A  
<187>Apr 21 14:30:25 149.49.77.11 -NoTag: -NoUTC 2009 425 1 mediaga-  
teway.g430 | 0 MSY-TRPMAJNA[VOICE-Error: No Call Controller Found,  
ID=N/A
```

power-down reset

Servicetechniker können mit diesem Befehl die Stromzufuhr der G450-Hauptkarte unterbrechen. Der Befehl ist nützlich, wenn an einer der Komponenten ein Hardwarefehler vorliegt und ein Warm-oder Kaltstart die Funktionalität nicht wieder herstellen kann.

Dieser Befehl entspricht Trennung und Neuanschluss des G450 mit der Hauptstromzufuhr oder dem Entfernen der G450-Hauptkarte und ihrem erneuten Einsetzen.

Hinweis:

Dieser Befehl gilt nur für die G450-Hauptkarte; möglicherweise liegt jedoch ein Ausfall der S8300-Konnektivität während des G450-Startvorgangs vor.

reset power-down

Syntax

```
reset power-down
```

Beschreibung

Verwenden Sie den Befehl für die Unterbrechung der Stromzufuhr, wenn die Stromzufuhr für G450 unterbrochen werden soll.

Benutzer-Level

admin

Kontext

allgemein

Beispiel

Ausführung eines Neustarts durch Unterbrechung der Stromzufuhr:

```
G450-001(super) # reset power-down
```

Hinweis:

Der Befehl ist nur verfügbar für G450 2.x oder darüber.

- Bei G450 Version 1.x, ist die Schaltfläche ASB rechts neben der Schaltfläche RST.
- Bei G450 Version 2.x, ist die Schaltfläche ASB über der Schaltfläche RST.



Hinweis:

Der Befehl führt zu einem Service-Ausfall.

Kapitel 3: SES-Änderungen

Dieses Kapitel gibt eine Übersicht über die Funktionen und Erweiterungen von Avaya Aura™ SIP Enablement Services (SES) Version 5.2.1.

Installation des Avaya S8800 Servers für SES

Siehe *Installing the Avaya S8800 Server for Avaya Aura™ SIP Enablement Services*, 03-603447, Ausgabe 1.

Migration von S8500 und S8510 Servern zum S8800 Server

Weitere Informationen über die neuesten Prozeduren finden Sie in Kapitel 5 von *Installing, Administering, Maintaining, and Troubleshooting Avaya Aura™ SIP Enablement Services*, 03-600768, Ausgabe 8.0.

SES Mixed-mode Trusted Host Interface

Die Funktion Trusted Origination Host wurde eingeführt, um das Problem mehrerer Benutzer auf einer IP-Adresse zu lösen, die alle versuchen, mit Avayas Komponenten über Transport Layer Security (TLS) zu kommunizieren und sich zu registrieren.

Die Prozeduren für das Hinzufügen und Bearbeiten von vertrauenswürdigen Hosts wurden verändert, damit die Option **Perform Originating Process** eingeschlossen ist, wobei Sie einen vertrauenswürdigen Host als Trusted Origination Host festlegen können.

Weitere Informationen zu den neuesten Prozeduren finden Sie unter *Installing, Administering, Maintaining, and Troubleshooting Avaya Aura™ SIP Enablement Services*, 03-600768, Ausgabe 8.0.

Kapitel 4: Communication Manager Messaging - Änderungen

Installation von Avaya Aura™ Communication Manager Messaging auf einem S8800 Server

Neue Serverunterstützung für Communication Manager Messaging

Konfigurieren Sie einen S8800 Server im Simplex-Modus, um Communication Manager Messaging zu installieren. [Installation von Communication Manager](#) auf Seite 63.



Hinweis:

Communication Manager Messaging kann nur auf einem Hauptserver konfiguriert werden. Ein S8800 Server auf dem Communication Manager Messaging installiert ist, unterstützt die Konfiguration auf einem LSP oder einem ESS-Server nicht.

Für alle anderen Aufgaben, die mit der Installation von Communication Manager Messaging auf einem S8800 Server in Verbindung stehen, siehe *Avaya Aura™ Communication Manager Messaging Installation and Initial Configuration* 03-603353.

Installation von Communication Manager Messaging

Installationshinweise für Communication Manager Messaging finden Sie unter [Installation von Communication Manager](#) auf Seite 63.

Sicheres Real-Time Transport Protocol (RTP)

Überblick

Das SRTP-Protokoll verschlüsselt nahtlos Audioströme für Anrufe über Communication Manager Messaging. Es ermöglicht AES-128-CM Verschlüsselung mit 32 und 80-Byte-Authentifizierung.



Hinweis:

TN2302-Medienprozessoren unterstützen SRTP nicht.

Anmeldung beim Communication Manager-Server mit PuTTY

Voraussetzungen

PuTTY-Anwendung

-
1. Öffnen Sie ein PuTTY-Fenster.
 2. Im Feld **Host Name (or IP address)** geben Sie die IP-Adresse des Communication Manager-Servers ein.
 3. Wählen Sie **SSH**.
 4. Klicken Sie auf **Open** (Öffnen).
-

Zugriff auf den Communication Manager Server

-
1. Geben Sie im Bildschirm SSH die Benutzerzugangsdaten für den `init`-Benutzer ein.
 2. Drücken Sie `Enter` für den Terminaltyp.
 3. Drücken Sie `y` oder `n`, um die Sessionpriorität festzulegen.
 4. Geben Sie `sat` ein.

5. Geben Sie das Kennwort für den "Init"-Benutzertyp an.
 6. Geben Sie `w2ktt` in der Eingabeaufforderung für Terminaltyp ein.
-

Ändern von Kundenoptionen, um Medienverschlüsselung zu ermöglichen

1. Melden Sie sich mit PuTTY beim Communication Manager-Server an.
 2. Auf dem Bildschirm SAT geben Sie `change system-parameters customer` (Ändern der Kunden-Systemparameter) ein.
 3. Setzen Sie auf Seite 4 das Feld **enable-Media Encryption** (Medienverschlüsselung aktivieren) auf `y`.
 4. Geben Sie `save trans` ein.
 5. Drücken Sie zum Beenden `Esc+X`.
-

Ändern von Signalisierungsgruppe, um Medienverschlüsselung zu ermöglichen

1. Auf dem Bildschirm SAT geben Sie `change signaling-group x` ein, `x` ist dabei die Nummer der Signalisierungsgruppe.
2. Vergewissern Sie sich, dass das Feld **media encryption** (Medienverschlüsselung) auf `y` steht.
3. Geben Sie das Kennwort im Feld **passphrase** ein.

 Hinweis:

Das Kennwort darf zwischen 8 und 30 Zeichen lang sein. Es darf Buchstaben und numerische Symbole, Buchstaben und Zahlen enthalten.

 Wichtig:

Merken Sie sich das Kennwort, das Sie im Feld **passphrase** einrichten. Damit SRTP funktioniert, stellen Sie das Kennwort auf der Webseite Switch Link Admin auf der Seite Messaging Web administration bereit.

Einrichten des IP-Codecsatzes

-
1. Geben Sie `change ip-codec-set x` ein, wobei `x` die Codecsatz-Nummer ist.
 2. Stellen Sie den SRTP-Typ auf `1-srtp-aescm128-hmac80`, `2-srtp-aescm128-hmac32` oder `none`.
-

Einrichten des SRTP-Typs auf der Communication Manager Messaging Verwaltungswebschnittstelle

-
1. In der System Management Interface unter **Administration** klicken Sie auf **Messaging**.
 2. Unter **Switch Link Administration** klicken Sie auf **Switch Link Admin**.
 3. Im Feld **Media Encryption** wählen Sie den gleichen SRTP-Typ, den Sie bereits im Bildschirm `change ip-codec-set` eingerichtet haben.
 4. Im Feld **Passphrase** geben Sie das Kennwort ein, das Sie im Bildschirm `change signaling-group` eingerichtet haben.
 5. Klicken Sie auf **Save**
-

Neustarten der Messaging-Anwendung

-
1. Klicken Sie unter **Utilities** auf **Stop Messaging** (Messaging stoppen).
 2. Wenn die Anwendung stoppt, klicken Sie auf **Start Messaging** (Messaging starten)
-

Aktivieren der Medienverschlüsselung für das Gateway

-
1. Geben Sie `change media-gateway x` ein, wobei `x` die Nummer des Mediengateways ist.
 2. Aktivieren Sie die Medienverschlüsselung für das Gateway
-

Zugriff auf Messaging für alle Nicht-SRTP kompatiblen Endpunkte zulassen

-
1. Mit PuTTY beim Communication Manager-Server anmelden.
 2. Zugriff auf Communication Manager-Server.
 3. Typ `Ändern des IP-Codecsatzes x`, `x` ist die Codecsatznummer.
 4. Legen Sie die Medienverschlüsselungswerte fest
 - i. `1-srtp-aescm128-hmac80` oder `2-srtp-aescm128-hmac32`
 - ii. `none`



Hinweis:

Wenn Sie möchten, dass sämtliche Kommunikation zwischen Messaging und Endpunkten über durchgehende Audioverschlüsselung verfügen, löschen Sie den Eintrag `none` (Keine) aus der Medienverschlüsselungsliste.

Aktualisieren von Avaya Aura™ Communication Manager Messaging

Aktualisieren von Communication Manager R5.1.x auf Communication Manager Messaging R5.2.1 auf einem S85XX Server

Aktualisieren Sie Communication Manager R5.1.x (ohne Communication Manager Messaging) auf Communication Manager R5.2.1. Wenn Sie den Server auf Communication Manager

ger R5.2.1 aktualisiert haben, befolgen Sie die gleiche Prozedur für die Installation von Communication Manager Messaging R5.2.1.

Aktualisieren von Communication Manager von R5.1 auf R5.2.1

-
1. Melden Sie sich bei der Webseite Maintenance Web Interface an.
 2. Klicken Sie unter **Server Upgrades** auf **Manage Software**.
 3. Wählen Sie auf der Seite Manage Software: Copy den Ort aus, von dem die Installation zu kopieren ist, und klicken Sie auf **Continue**.
 4. Wählen Sie die Version **05.2.1-xxx.xxx.x** aus, und klicken Sie auf **Continue**.
 5. Wählen Sie die Option **Install one of the following releases resident on the local hard drive**, und klicken Sie auf **Continue**.
 6. Wählen Sie die Version **5.2.1.xxx.xxx**, und klicken Sie auf **Continue**.
 7. Wählen Sie auf der Seite Choose license source die Option **I want to reuse the license files from the currently active partition on this**.
 8. Wählen Sie **Update authentication information as well as license information**.
 9. Klicken Sie auf **Continue**, und fahren Sie mit der Installation von Communication Manager fort.
-

Installation von Communication Manager Messaging R5.2.1

-
1. Melden Sie sich bei der Webseite System Management Interface (System Management-Schnittstelle) an.
 2. Im Menü **Upgrade** (Aktualisieren) klicken Sie auf **Manage Software**.
 3. Wählen Sie auf der Seite Manage Software: Copy **yes**, um die Communication Manager Messaging-Software zu kopieren.
 4. Klicken Sie auf **Continue**.
 5. Fahren Sie mit der Installation von Communication Manager Messaging fort.
-

LDAP (Lightweight Directory Access Protocol)

Überblick

Lightweight Directory Access Protocol (LDAP) ist eine Datenbank, die Systemdaten, Abonentendaten und die Dienstklasse für den einzelnen Abonnenten enthält. Kunden wünschen Zugriff auf die Abonentendatenbank, damit sie Daten in großem Maßstab verwalten können. Standard-LDAP-Clients wie Microsoft Outlook sind Clients, die beim Zugriff auf die LDAP-Datenbank unterstützt werden.

**Hinweis:**

LDAP enthält keine Mailbox-Daten wie Nachrichten, Begrüßungen und Ansagen.

Verbinden zu LDAP

Ein Kunde kann auf zweierlei Weise Verbindung zu LDAP herstellen:

- Anonym
- Als vertrauenswürdiger Server

Nehmen Sie Verbindung zur LDAP-Datenbank über eine anonyme Verbindung auf, geben Sie dafür eine IP-Adresse und einen eindeutigen Namen an. Bei dieser Art Verbindung erhält man begrenzte Informationen von der Datenbank. Ein Kunde verwendet diese Verbindung, um Daten zu lesen.

Nehmen Sie als vertrauenswürdiger Server Verbindung zur LDAP-Datenbank auf, geben Sie einen vertrauenswürdigen Servernamen, eine IP-Adresse des Kunden und ein Kennwort an. Dieser Verbindungstyp wird verwendet, um Abonnenten in großer Zahl zu verwalten. Kunden können die Zugangsdaten von Avaya nutzen, um eine Verbindung herzustellen und Informationen über Abonnenten zu erhalten.

LDAP-Prozesse

Die Webseite [LDAP Status/Restart](#) auf der Schnittstelle für die Nachrichtenverwaltung listet die Prozesse auf:

- **slapd**-Prozess, ist verantwortlich für das Funktionieren von LDAP.
- **Ldapfe**-Prozess, verarbeitet Anfragen von Clients über Abonnenteninformationen und entscheidet, wie Anfragen verfolgt werden. Er führt die Webverwaltungsanfragen für die Benutzer der Webseite Messaging aus.
- **Ldapcorp** -Prozess, entspricht Ldapfe-Prozess, außer dass Ldapcorp die externe Verwaltung ermöglicht; Kunden greifen auf die LDAP-Datenbank außerhalb der Audix-Domain zu.

Statusüberprüfung der LDAP-Prozesse

1. Auf der Webseite System Management Interface (System Management-Schnittstelle) klicken Sie im Menü **Administration** auf **Messaging**.
2. Klicken Sie unter **Utilities** auf **LDAP Status / Restart**.
3. Prüfen Sie, ob alle Prozesse laufen.
4. Wenn die Prozesse nicht laufen, klicken Sie auf **Restart**, um die Prozesse manuell zu starten.



Hinweis:

Sie müssen die Messaging-Anwendung erneut starten, um alle LDAP-Prozesse zu starten.

Login-Profilinfrastruktur

Überblick

Sie können ein Benutzer-basiertes Profil erstellen und einem vorhandenen Communication Manager-Profil oder einem benutzererstellten Communication Manager-Profil zuordnen.

Die Communication Manager Messaging-Anwendung verwendet die Benutzer-basierten Profile wie sie in Communication Manager erstellt wurden. Vom Benutzer definierte Profile ermöglichen es Ihnen, einem Benutzer nur den Zugriff auf einen bestimmten Satz Verwaltungswebseiten zu gewähren.

Sie können beispielsweise ein Login Account erstellen und das Profil des berechtigten Administrators zu ordnen (sa). Standardmäßig ist es Communication Manager-Profil 18 zugewiesen. Dieses Profil gewährt Zugriff, der dem Kunden-Login Super-User entspricht. Das

Administratorprofil ohne Privilegien (vm) ist Communication Manager-Profil 19 zugewiesen. Dieses Profil gewährt Zugriff, der dem Kunden-Login Nicht-Super-User entspricht.

Erstellen eines Benutzer-basierten Profils

-
1. Melden Sie sich bei der Webseite System Management Interface (System Management-Schnittstelle) an.
 2. Klicken Sie im Menü **Administration** auf **Server (Maintenance)** (Serverwartung).
 3. Klicken Sie unter **Security** (Sicherheit) auf **Web Access Mask** (Maske Webzugriff).
 4. Klicken Sie auf **Add** (Hinzufügen).
 5. Geben Sie eine Profilnummer ein, die Sie für die Benutzer anlegen wollen.

**Hinweis:**

Sie können Profile zwischen 20 und 69 erstellen. Die Profile 0-19 sind reserviert.

6. Wählen Sie **Create** (Erstellen), und richten Sie alle Werte ein, um den Zugriff zu ermöglichen.
7. Klicken Sie auf **Submit** (Senden).
8. Wählen Sie das Profil aus.
9. Klicken Sie auf **Change** (Ändern).
10. Standardmäßig werden alle Webseiten ausgewählt. Wählen Sie die Webseiten aus, auf die ein Benutzer Zugriff haben muss.
11. Klicken Sie auf **Submit** (Senden).

**Hinweis:**

Sie können auf der Webseite Change Access Masks (Ändern der Zugriffsmasken) nur Communication Manager Messaging-Webseiten ansehen, wenn die Messaging-Anwendung installiert ist.

Zuweisen eines Profils zu einem Benutzer

-
1. Melden Sie sich bei der Webseite System Management Interface (System Management-Schnittstelle) an.
 2. Klicken Sie im Menü **Administration** auf **Server (Maintenance)** (Serverwartung).

3. Klicken Sie unter **Security** (Sicherheit) auf **Administration Accounts** (Administratorkonten).
 4. Wählen Sie **Add Login** (Login-ID hinzufügen) aus.
 5. Wählen Sie den Profiltyp.
 6. Klicken Sie auf **Submit** (Senden).
-

Sichern und Wiederherstellen von Communication Manager Messaging-Daten

Überblick

Communication Manager Messaging unterstützt bis zu 6000 Mailboxen. Das Sichern von Communication Manager Messaging-Daten kann leicht 50 Gigabyte oder mehr erreichen. Es wäre für Kunden ungewöhnlich, die Übertragung einzelner Dateien dieser Größe zu unterstützen. Daher besteht Communication Manager Messaging-Datensicherung aus mehreren Dateien und jede ist klein genug, um in einer Kundenumgebung übertragen zu werden.

Unterstützte Sicherungsmethoden:

- FTP
- SFTP
- SCP
- Compact PC-FlashCard



Wichtig:

Avaya empfiehlt das Sichern der Daten auf einem Netzwerkservers.

Sichern von Communication Manager Messaging-Daten

Voraussetzungen

Die Sicherung der Daten erfolgt über Netzwerkservers oder eine PC-Karte.

-
1. Melden Sie sich bei der Webseite System Management Interface (System Management-Schnittstelle) an.
 2. Wählen Sie **Specify Data Sets** (Datensätze angeben).

3. Wählen Sie **Communication Manager Messaging (CMM)**.
4. Wählen Sie **Translations, Names, and Messages** (Konfigurationsdaten, Namen und Nachrichten).
5. Wählen Sie die Sicherungsmethode.
6. Legen Sie ein Kennwort fest, um die Sicherungsdaten zu verschlüsseln.
7. Geben Sie einen Wert von 1 bis 200 an, um die Größe der übertragbaren Datei über das Netzwerk zu begrenzen, damit eine erfolgreiche Sicherung der Communication Manager Messaging-Daten gewährleistet ist.

Der angegebene Wert im Feld **Download size** (Download-Größe) für das Kästchen mit den Communication Manager Messaging-Daten für den Transfer, sollte kleiner oder gleich der maximal im Netzwerk zulässigen Dateiübertragungsgröße sein. Das resultierende Sicherungsbild umfasst eine oder mehrere Dateien, die die angegebene Größe nicht überschreiten. Wenn Sie beispielsweise den Wert auf 5 eingerichtet haben, ist die Größe der Daten 500 MB.

8. Klicken Sie auf **Start Backup** (Sichern starten).

Communication Manager Messaging-Anwendung lädt und verarbeitet alle Sicherungsdateien nacheinander bevor die nächste Sicherungsdatei im Datensatz heruntergeladen wird.



Wichtig:

Der Sicherungsdatensatz kann mehrere Sicherungsdateien umfassen (tar-Dateien). Nur die Meta-Tar-Datei (Backup-Datei) ist auf der Webseite View / Restore Data (Daten ansehen / wiederherstellen) sichtbar.



Hinweis:

Communication Manager Messaging kann die Daten früherer Versionen wiederherstellen.

Aktualisierungen von Dokumentation und Verfahren für Communication Manager Messaging R5.2

Ändern der Systemparameter – Weiterleitung

Im Abschnitt *system parameters coverage* der Dokumentation *Avaya Aura™ Communication Manager Messaging Installation and Initial Configuration, 03-603353* :

Auf dem Bildschirm *system-parameters coverage-forwarding* (Systemparameter – Weiterleitung/Rufumleitung) muss das Feld **Threshold for Blocking Off_Net Redirection of Incoming Trunk Calls** auf **1** gesetzt werden.

Ändern der Berechtigungsklasse

Sie müssen eine Sammelgruppe für Messaging erstellen, bevor Sie die Berechtigungsklasse ändern können. Siehe Seite 50 in *Avaya Aura™ Communication Manager Messaging Installation and Initial Configuration, 03-603353* .

-
1. Geben Sie auf dem Bildschirm `SAT change cor x`, ein wobei *x* die Nummer der Berechtigungsklasse ist.
 2. Aktualisieren Sie das Feld **Calling Party Restriction** (Anrufannahmesperren) auf `none` (Keine). Der Standard für das Feld ist `Outward`.

 Hinweis:

Sie können die Anrufsperrung für abgehende Verbindungen einsetzen, um Benutzer zu hindern, Anrufe in einem öffentlichen Netzwerk zu machen. Diese Benutzer können noch andere Telefonnutzer und die Telefonzentrale anrufen und über Querverbindungen telefonieren. Gegebenenfalls können die Telefonzentrale oder ein Nutzer eines uneingeschränkten Telefons einen Anruf für einen Telefonnutzer mit Anrufssperren an eine externe Nummer tätigen. Anrufe, die in eine Amtsleitung kommen, werden abgelehnt, wenn das Feld Anrufssperre auf dem Bildschirm *Class of Restriction* (Berechtigungsklasse) auf `Outward` (abgehende Verbindung) eingerichtet ist.

Kapitel 5: Communication Manager Installation auf S8800 Server

Installation und Konfiguration von Avaya Aura™ Communication Manager

Überblick

Communication Manager unterstützt den S8800 Server in einem 1U-Modell. Sie können Communication Manager auf einem S8800 Server in einem 1U-Modell entweder in Simplex- oder Duplex-Modus konfigurieren.



Hinweis:

Communication Manager im Simplex-Modus auf dem S8800 Server konfiguriert gleich einem S85XX Server, und bei der Konfiguration im Duplex-Modus einem S87XX Server.

Installation von Communication Manager

Voraussetzungen

Communication Manager-Installations-CD-ROM

Greifen Sie in einer Telnet-Session auf die Information auf der CD-ROM zu.

-
1. Klicken Sie auf Ihrem Service-Laptop auf **Start > Run**, um das Dialogfeld Run (Ausführen) zu öffnen.
 2. Geben Sie `telnet 192.11.13.6` ein, und drücken Sie auf `Enter`, um den ersten Bildschirm zu sehen.
 3. Wählen Sie **Install**, vergewissern Sie sich, dass **OK** ausgewählt ist, und drücken Sie **Enter**.
 4. Auf dem Bildschirm **Select Release Version** vergewissern Sie sich, dass **Build line** und **OK** ausgewählt sind und drücken `Enter`.

5. Auf dem Bildschirm **Select Server Mode** vergewissern Sie sich, dass **server mode type** und **OK** ausgewählt sind und drücken **Enter**.
6. Je nach dem gewählten Serverdopplungsmodus werden unterschiedliche Bildschirme angezeigt.
 - Im Simplex-Modus wählen Sie **messaging option** und **OK** und drücken **Enter**.
 - Im Duplex-Modus wählen Sie **Yes**, um den Server sowohl für Steuerungsnetzwerk A als auch B zu konfigurieren und drücken **Enter**.

Erhöhen und Verringern der Verfügbarkeit des S8800 Servers

Wenn Sie den S8800 Server im Simplex-Modus konfigurieren und die Verfügbarkeit erhöhen möchten, indem Sie ihn zu einem Duplex-Server machen, müssen Sie die Communication Manager-Software neu installieren. Wählen Sie während der Installation den Server-Modus als Duplex. Wenn Sie jedoch die Server-Verfügbarkeit in Duplex geändert haben, können Sie Communication Manager Messaging nicht installieren, denn es kann nicht auf einem Server in Duplex-Modus installiert werden.

Wenn Sie den S8800 Server im Duplex-Modus konfigurieren und die Verfügbarkeit verringern möchten, indem Sie ihn zu einem Simplex-Server machen, müssen Sie die Communication Manager-Software neu installieren. Wählen Sie während der Installation den Server-Modus als Simplex.

Sie finden Informationen bezüglich der Hardware eines S8800 Server unter *Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager document, 03-603444*, Ausgabe 1.

Zugehörige Aufgaben während der Installation eines S8800 Servers im Simplex-Modus finden Sie unter *Installing and Configuring the Avaya S8500-Series Server document, 03-300143*.

Zugehörige Aufgaben während der Installation eines S8800 Servers im Duplex-Modus finden Sie unter *Installing and Configuring the Avaya S8700-Series Server document, 03-300145*.

Konfiguration des Servers

Wenn Sie einen S8800 Server im Simplex-Modus konfigurieren möchten, schauen Sie unter *Installing and Configuring the Avaya S8500-Series Server document, 03-300143*.

 Hinweis:

Wenn Sie sich bei der Konfiguration nach diesem Dokument richten, ignorieren Sie die Webseite Configure RMB, denn sie trifft für den S8800 Server im Simplex-Modus nicht zu. Außerdem ignorieren Sie die Hinweise auf SAMP in diesem Dokument, da der S8800 Server keine SAMP-Karte hat.

Wenn Sie einen S8800 Server im Duplex-Modus konfigurieren möchten, schauen Sie unter *Installing and Configuring the Avaya S8700-Series Server document, 03-300145*.

 Hinweis:

Wenn Sie sich bei der Konfiguration nach diesem Dokument richten, ignorieren Sie die Webseite Configure Switches, denn sie trifft für den S8800 Server im Duplex-Modus nicht zu.

Überwachung des Status des S8800 Server

Der Status von Communication Manager und S8800 Server kann über die Konfiguration der Communication Manager-Heartbeat-Trip und des Baseboard Management Controller (BMC) auf dem Server überwacht werden. Die Communication Manager-Heartbeat-Trip benötigt eine IP-Adresse, um die Heartbeats an SAL zu versenden sowie ein Kennwort zur Kontrolle des Zugriffs von Communication Manager auf SAL. Der BMC benötigt die IP-Adresse des Standard-Gateways um den Traffic von der BMC-Schnittstelle nach SAL zu verfolgen.

Verwalten Sie die folgenden Parameter auf Communication Manager um Communication Manager an SAL Heartbeat zu unterstützen:

- SALIP-Adresse
- Community-String
- IP-Adresse, die BMC nutzen soll
- Gateway-Adresse
- Subnet-Mask

Zugriff auf die Webseite „Configure Health Monitor“ (Statusüberwachung konfigurieren)

-
1. Öffnen Sie das System Management Interface.
 2. Im Menü **Administration** klicken Sie auf **Server (Maintenance)**.
 3. Unter **Server Configuration** (Serverkonfiguration) klicken Sie auf **Configure Health Monitor**.
-

Konfiguration von Communication Manager und Serverstatusparametern

1. Füllen Sie die Felder auf der Webseite Configure Health Monitor aus.
2. Klicken Sie auf **Change** (Ändern).

S8800 Ethernet-Portzuordnungen

	Simplex		Duplex		
	Steuerungsnetzwerk A und Kunden-/Unternehmens-LAN kombiniert	Unabhängiges Steuerungsnetzwerk A und Kunden-/Unternehmens-LAN	Steuerungsnetzwerk A und Kunden-/Unternehmens-LAN kombiniert	Unabhängiges Steuerungsnetzwerk A und Kunden-/Unternehmens-LAN	NIC - Standort
Ethernet 1 (Eth0)	Steuerungsnetzwerk A/ Kunden-/ Unternehmens-LAN	Steuerungsnetzwerk A	Dopplungs-Link		Befindet sich auf der Hauptplatine
Ethernet 2 (Eth1)	Service-Laptop		Service-Laptop		Befindet sich auf der Hauptplatine
Ethernet 3 (Eth2)	Nicht belegt		Steuerungsnetzwerk A/ Kunden-/ Unternehmens-LAN	Steuerungsnetzwerk A	Befindet sich auf dem speziellen Tochter-Board

	Simplex		Duplex		
	Steuerungsnetzwerk A und Kunden-/Unternehmens-LAN kombiniert	Unabhängiges Steuerungsnetzwerk A und Kunden-/Unternehmens-LAN	Steuerungsnetzwerk A und Kunden-/Unternehmens-LAN kombiniert	Unabhängiges Steuerungsnetzwerk A und Kunden-/Unternehmens-LAN	NIC - Standort
Ethernet 4 (Eth3)	Steuerungsnetzwerk B (sofern verwendet)		Steuerungsnetzwerk B (sofern verwendet)		Befindet sich auf dem speziellen Tochter-Board
Ethernet 5 (Eth4)	Nicht belegt	Kunden-/Unternehmens-LAN	Nicht belegt	Kunden-/Unternehmens-LAN	Befindet sich auf PCI Dual NIC-Board
Ethernet 6 (Eth5)	Nicht belegt		Nicht belegt		Befindet sich auf PCI Dual NIC-Board

Der Link **Set Identities** auf der Webseite **Configure Server** (Server konfigurieren) zeigt die Standard-Ethernet-Ports an, die jeder Art von Netzwerk zugeordnet sind. Für den S8800 Server im Duplex-Modus wird standardmäßig das Serverdopplungs-Link dem Ethernet 0-Port zugeordnet. Sie können in Abhängigkeit von der Netzwerkkonfiguration einen anderen Ethernet-Port wählen.

Verbesserungen der Softwaredoppelung

Softwaredoppelung liefert eine Speichersynchronisierung zwischen einem aktiven und einem Standby-Server, ohne dass Dopplungskarten der Serien DAL oder DAJ erforderlich sind. Softwaredoppelung ist in S88001U Server die Standardkonfiguration. Für Softwaredoppelung werden Doppelungsmeldungen über den Serverdopplungs-TCP/IP-Link versendet.

Avaya unterstützt weiterhin die vorhandenen Hardware-duplizierten S8710, S8720 und S8730 Server. Software-duplizierte S88001U Server besitzt die gleiche Anrufperformance wie der vorhandene Hardware-duplizierte Server der Serie S8700. Zur Konfiguration von Software-

doppelung in S88001U Server empfiehlt Avaya einen dedizierten Doppelungslink mit den folgenden Bandbreitenparametern zu verwenden:

- 1 GBit/s Raw-Link-Kapazität
- 50 MBit/s reservierte Bandbreite
- 8 ms Umlaufzeitverzögerung oder weniger
- 0,1 % Umlaufzeitpaketverlust oder weniger

Zur Konfiguration von Softwaredoppelung in S88001U Server, verwenden Sie den Assistenten **Configure Server** in System Management Interface (SMI).

IP-Schnittstelle für H.248-Gateways

Prozessor-Ethernet-IP-Schnittstelle

Prozessor-Ethernet (PE) ist eine logische Schnittstelle in Communication Manager. Es ist keine zusätzliche Hardware erforderlich, um PE zu implementieren. Es funktioniert wie C-LAN und kann anstelle von C-LAN in einer Netzwerkumgebung verwendet werden. Netzwerkkonfigurationen können sowohl PE als auch C-LAN verwenden.

PE kann auf Hauptservern und ESS-Server verwendet werden (Simplex und Duplex). Es ermöglicht die Verbindung zu verschiedenen IP-Geräten, wie H.323-Telefone, Amtsleitungen, Gateways, SIP-Amtsleitungen, H.248-Gateways und ausgewählten über IP verbundene Zusatzgeräte. Der von PE unterstützte Verkehr entspricht dem Verkehr, der von C-LAN unterstützt wird.

Siehe auch *Avaya Aura™ Communication Manager System Capacities Table for Release 5.2.1 document* wenn Sie die Anzahl der IP-Geräte wissen möchten, die für einen S8800 Server im Simplex und Duplex-Modus unterstützt werden.

Zuweisen der IP-Adresse zu Prozessor-Ethernet

-
1. Auf der Webseite Configure Server klicken Sie auf **Configure Interfaces** (Schnittstellen konfigurieren).
 2. Geben Sie die Prozessor-Ethernet IP-Adresse an.

 Hinweis:

Prozessor-Ethernet nutzt die Unternehmens-LAN IP-Adresse mit. Jeder Server in einem duplizierten System benötigt seine eigene Prozessor-Ethernet IP-Adresse.

Aktivierung von Prozessor-Ethernet

-
1. Öffnen Sie einen SAT-Bildschirm, geben Sie `change ip-interface procr` ein.
 2. Gehen Sie zum Feld **Enable Interface?** und setzen Sie es auf `y`.
 3. Vergewissern Sie sich, dass die Felder **Allow H.323 Endpoints?** und **Allow H.248 Gateways?** auf `y` gesetzt wurden.
 4. Geben Sie „`Save trans`“ ein..
-

Zuweisen der IP-Adresse für Prozessor-Ethernet auf der System Management-Schnittstelle

-
1. Öffnen Sie System Management Interface. (SMI).
 2. Im Menü **Installation** klicken Sie auf **Configure Server**.
 3. Fahren Sie fort damit, Serverdienste zu konfigurieren.
 4. Klicken Sie auf **Set Identities**, um den Ethernet-Port für Processor Ethernet zu konfigurieren.

 Hinweis:

Weisen Sie dem Prozessor-Ethernet und dem Unternehmens-LAN den gleichen Ethernet-Port zu.

5. Klicken Sie auf **Continue** (Weiter).
 6. Weisen Sie im Bildschirm Configure Interfaces die IP-Adresse für die Prozessor-Ethernet-Schnittstelle zu.
-

Konfiguration von Secure Access Link (SAL)

Konfigurieren von SAL-Gateway

Detaillierte Informationen wie das SAL-Gateway konfiguriert wird, finden Sie unter *Secure Access Link 1.8 SAL Gateway Implementation Guide*, Mai 2009.

Postinstallation

Aktivieren von Alarm an INADS über SAL

Communication Manager generiert nur dann Alarm über das SAL-Gateway wenn Communication Manager seine SNMP-Traps an das SAL-Gateway richtet.

Detaillierte Informationen über das Aktivieren von Alarm für das SAL-Gateway finden Sie unter: *Secure Access Link 1.8 SAL Gateway Implementation Guide*, Appendix, Product Alarm Configuration section, Mai 2009.

Installationsüberprüfung

Verbindung zum Server mit SAL

Sie finden detaillierte Informationen über die Verbindung zum Server mit SAL-Gateway unter *Secure Access Link 1.8 SAL Gateway Implementation Guide*, Mai 2009.

Kapitel 6: Hardware

Dieses Kapitel gibt Ihnen einen Überblick über die Hardware-Ergänzungen zu Version 5.2.1 von Avaya Aura™ Communication Manager.

Digitaltelefone der Serien Avaya 14xx

Die Digitaltelefone der Serien Avaya 14xx, vor allem 1408 und 1416, sind Digital Communications Protocol-(DCP)-Telefone. Diese Digitaltelefone erhalten den Aliasnamen oder werden verwaltet als Avaya 24xx Digitaltelefone.

Die Digitaltelefone der Serien Avaya 14xx verfügen über folgende Eigenschaften:

- Einstellbarer Display-Neigungswinkel
- Wandmontage
- Telefonhörer und Tastenfeld
- Gut sichtbare Nachrichtenanzeige
- Drei oder vier LCD-Leitungen
- Navigationstasten: Beenden, OK und Telefon
- Tasten für Konferenz, Umlegen, Trennen, Halten und Wahlwiederholung
- Telefon- und Kontaktetasten
- 8 oder 16 Funktionstasten
- Tasten für Lautsprecher, Sprechgarnitur und Stummschaltung (jeweils mit LED)
- Lautstärkeregelungstasten für:
 - Telefonhörer
 - Sprechgarnitur
 - Speakerphone
- Herunterladen von Firmware-Upgrades
- Vier Softkey-Funktionstasten
- Anrufprotokolltaste (zur Prüfung aller eingegangenen beantworteten, unbeantworteten und abgehenden Anrufe)
- Taste zum zügigen Aufrufen der Voicemail
- Eine (Avaya-Menü) Taste (zur Anpassung der Einstellungen)

- Rufumleitung, Follow-me-Funktionen
- Navigationspfeile

Avaya S8800 Server - Übersicht

Einleitung

Der S8800 Server unterstützt verschiedene Avaya Softwareanwendungen. Der Server ist als 1U-Modell oder 2U-Modell und mit verschiedenen Hardwarekomponenten erhältlich. Das Servermodell und die spezifischen Hardwarekomponenten im Server hängen von den Erfordernissen der Softwareanwendung ab, die darauf ausgeführt wird.

Communication Manager unterstützt das Modell 1U der S8800 Server. Bei der Installation von Communication Manager im Simplex-Modus auf dem S8800 Server, verwenden Sie nur 1 S8800 Server, während Sie bei der Installation von Communication Manager im Duplex-Modus 2 S8800 Server benötigen.

Verwandte Themen:

[Serverfront](#) auf Seite 76

[Server Rückseite](#) auf Seite 77

[Serverspezifikationen](#) auf Seite 78

[Serverkomponenten](#) auf Seite 80

[Umgebungsvoraussetzungen](#) auf Seite 82

Kapitel 7: Dokumentations- und Verfahrensaktualisierungen

Die Communication Manager-Dokumente (Wartungsalarm, Befehle, Prozeduren, Hardware-dokumentation, Administrator Guide, usw.) werden für diese Version nicht aktualisiert.

Dieses Kapitel beschreibt die folgenden Updates für Communication Manager Version 5.2.1, die für diese Version nicht dokumentiert werden.

Verwandte Themen:

[Administration für das Avaya G450 Media Gateway](#) auf Seite 73

[Administrator Guide](#) auf Seite 73

[Funktionsbeschreibung und Implementierung](#) auf Seite 74

[Hardwarebeschreibung und -übersicht](#) auf Seite 75

[Screen Reference](#) auf Seite 82

Administration für das Avaya G450 Media Gateway

Folgende Änderungen treffen für *Administration for the Avaya G450 Media Gateway*, 03-602055, zu:

DHCP-Server CLI-Konfiguration

Reference 5.2 Version – Kapitel 18, Schritt 3, Seite 484: Die kombinierte Anzahl IP-Adressen in allen Pools darf 1024 Adressen nicht übersteigen und nicht 256 Adressen.

Administrator Guide

Für *Administering Avaya Aura™ Communication Manager*, 03-300509 gelten folgende Änderungen:

Avaya Site Administration

Übersicht 5.2 Version – Seite 20 und Seite 545, erster Absatz, der folgende Satz wurde entfernt: ASA ist in mehreren Sprachen verfügbar.

Telefonfunktionstasten

Eine Taste für sofortiges Weiterleiten wurde der Tabelle Telefonfunktionstasten hinzugefügt.

Tastenbe-schriftung	Tasten-name	Beschreibung
Sofortiges Weiterleiten	Inst-trans	Die Taste „Sofort Weiterleiten“ leitet umgehend weiter, indem sie einen unüberwachten Transfer zum der Taste zugeordneten Ziel vornimmt. Die Taste „Sofort weiterleiten“ ist für die Weiterleitung an Polycom-Raumsysteme gedacht, die in der Lage sind, eine Konferenz sowie Auto-Antwortanrufe zu unterstützen. Die Taste „Sofort weiterleiten“ ist nicht auf Video-Set-Typen beschränkt; sie kann auch für andere Set-Typen nützlich sein.

Funktionsbeschreibung und Implementierung

Folgende Änderungen betreffen *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555–245–205:

Verwaltung von Nebenstelle zu Mobiltelefon

Einrichten der One-X Server-Integration

-
1. Richten Sie eine SIP-Signalisierungsgruppe und ein Amtsleitungsbündel zwischen Communication Manager und one-X Server ein.
 2. Benutzer bereitstellen mit Communication Manager-Nebenstellen auf one-X Server.
 3. Bereitgestellte Benutzer werden über ONE-X Zuordnung(en) verfügen, die in Abhängigkeit von ihren Nebenstellen auf Communication Manager erworben wurden.

den. Überprüfen Sie mit `list off-pbx-telephone station-mapping` oder `display off-pbx-telephone station-mapping` **Befehl:**

Bridged Call Appearance (Interaktionen für Leitungstastenkopie)

Notrufe

Wenn ein Benutzer einen Notruf von einer Leitungstastenkopie wählt, basiert die Calling Party Number (Rufnummer des Anrufers), die an die Notrufzentrale gesendet wird, auf der Nebenstelle des physischen Telefons, von dem der Anruf getätigt wird.



Hinweis:

Wenn Sie einen Notruf machen möchten, müssen Sie mindestens eine Leitungstaste als primäre Leitungstaste einrichten.

Interaktionen für Whisper Paging

Aufschaltfunktion

Wenn ein Serviceüberwacher bei einem Anruf aktiv ist, wird Whisper Paging einer beobachtenden oder beobachteten Nebenstelle verweigert.

Hardwarebeschreibung und -übersicht

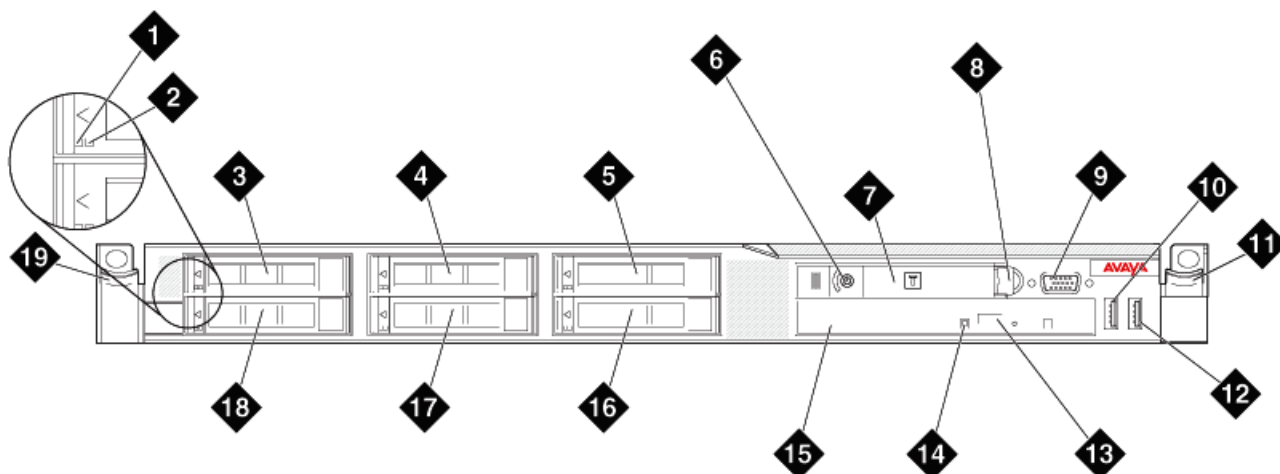
Folgende Änderungen betreffen *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207:

TN791 „Analog Guest Line“ (Gast-Analogleitung) – 16 Ports

Der Hinweis, dass die TN791 Baugruppe im G650 Media Gateway nicht verwendet wird, wurde entfernt.

Avaya S8800 Server

Serverfront



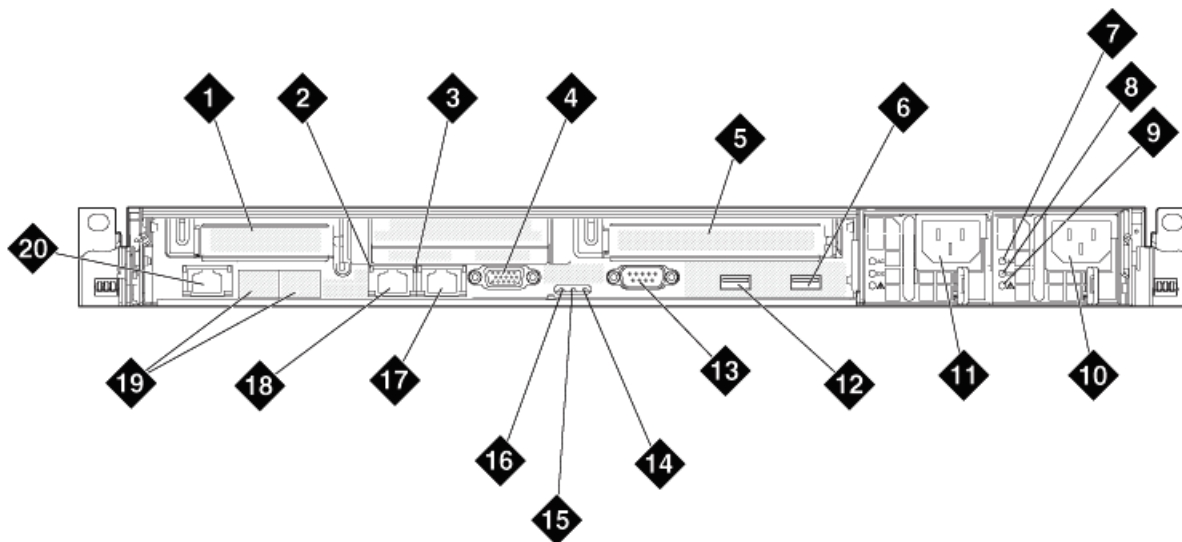
hw881fn LAO 092209

1	Festplatten-LED (grün)
2	Festplattenstatus-LED (bernsteinfarben)
3	Laufwerkseinschub 0
4	Laufwerkseinschub 2 (bei Communication Manager nicht genutzt)
5	Laufwerkseinschub 2 (nicht genutzt bei Communication Manager)
6	Schalter für Leistungssteuerung und LED
7	Informationsfeld für die Telefonzentrale * Hinweis: Das Informationsfeld für Telefonzentrale wird in der eingeschobenen Position gezeigt.
8	Entriegelung am Informationsfeld für die Telefonzentrale
9	Videoanschluss
10	USB-Anschluss 1
11	Rackentriegelung
12	USB-Anschluss 2
13	DVD-Auswurfstaste
14	Betriebs-LED für das DVD-Laufwerk
15	DVD-Laufwerk

16	Laufwerkseinschub 5 (bei Communication Manager nicht genutzt)
17	Laufwerkseinschub 3 (bei Communication Manager nicht genutzt)
18	Laufwerkseinschub 1
19	Rackentriegelung

Verwandte Themen:

[Einleitung](#) auf Seite 72

Server Rückseite

hw881bk LAO 100809

1	PCIe-Steckplatz 1 (Niedrigprofil PCI-Steckplatz) belegt mit DUAL NIC-Tochterkarte, liefert Ethernet 5 (eth4) und Ethernet 6 (eth5). * Hinweis: Ethernet-Anschluss 6 (eth 5) nicht verwendet bei Communication Manager R 5.2.1.
2	Ethernet-Betriebs-LED
3	Ethernet-Link-LED
4	Videoanschluss
5	PCIe-Steckplatz 2
6	USB-Anschluss 4
7	Wechselstrom-LED (grün)
8	Gleichstrom-LED (grün)
9	Netzteilfehler-LED (bernsteinfarben)

10	Netzteil 2 (optional redundantes Netzteil)
11	Netzteil 1 (primäres Netzteil)
12	USB-Anschluss 3
13	Serieller Anschluss
14	Systemfehler-LED (bernsteinfarben)
15	System-Locator-LED (blau)
16	Betriebs-LED (grün)
17	Ethernet-Anschluss 2 (eth 1)
18	Ethernet-Anschluss 1 (eth 0)
19	Ethernet-Anschlüsse 3 (eth 2) und 4 (eth 3)
20	Systemmanagement-Ethernet-Anschluss (IMM)



Hinweis:

Hardwarebezeichnung für Ethernet-Ports auf dem Server wird Ethernet-Anschlüsse genannt. Communication Manager Software verweist auf die Ethernet-Ports als eth.

Verwandte Themen:

[Einleitung](#) auf Seite 72

Serverspezifikationen

Typ	Beschreibung
Maße	Höhe: 43 mm (1,69 Zoll, 1U) Tiefe: 711 mm (28 Zoll) Breite: 440 mm (17,3 Zoll)
Gewicht	Höchstgewicht: 15,4 kg (34 lb.) bei voller Konfiguration.
Wärmeleistung	Geschätzte Wärmeleistung: • Mindestkonfiguration: 662 Btu pro Stunde (194 Watt) • Höchstkonfiguration: 1400 Btu pro Stunde (400 Watt) Wärmeleistung variiert, je nach Anzahl und Art der optionalen Funktionen, die installiert wurden und der optionalen Strommanagementfunktionen, die verwendet werden.
Lärmemissionen	Deklarierte Schallleistung, im Betrieb: 6,1 Bel Schalllevel werden in kontrollierten akustischen Umgebungen gemessen, entsprechend der von American National Standards Institute (ANSI) spezifizierten Verfahren S12.10

Typ	Beschreibung
	und ISO 7779, und werden in Übereinstimmung mit ISO 9296 protokolliert. Die tatsächlichen Schalldrucklevel in einer gegebenen Umgebung können aufgrund von Raumreflektionen und anderen nahegelegenen Geräuschquellen die genannten Durchschnittswerte übersteigen. Die angegebenen Schallkraftlevel zeigen eine Obergrenze an, unter der eine Vielzahl Computer arbeiten.
Anforderungen an die elektrische Leistungsaufnahme	• Sinusförmiges Eingangssignal benötigt (47 – 63 Hz) • Eingangsspannung unterer Bereich: - Min. 100 V~ - Max. 127 V~ • Eingangsspannung oberer Bereich: - Min. 200 V~ - Max. 240 V~ • Eingangsleistung in Kilovolt-Ampere (kVA) (ca.): - Minimum: 0,194 kVA - Maximum: 0,700 kVA
Anschlüsse auf der Vorderseite	• Zwei USB • Video
Anschlüsse auf der Rückseite	• Zwei Ethernet (RJ 45). Optional zwei oder vier zusätzliche Ethernet. • Seriell • Zwei USB • Video • Systemmanagement-Ethernet (IMM)

Verwandte Themen:

[Einleitung](#) auf Seite 72

Serverkomponenten

Komponente	Mindestanforderung	Upgrade-Optionen basierend auf Produktanforderungen
Mikroprozessor	Ein Intel E5520 Quad Core, 2,26 GHZ-Prozessor	Keine Zusatzoptionen
Arbeitsspeicher	4 GB von 1333 MHZ, voll gepufferte DDR-3 RDIMMs (Zwei 2GB DIMMs):	Keine Zusatzoptionen
Medienlaufwerk	DVD-R/W SATA-Slim-line	Keine Zusatzoptionen
Festplattenlaufwerk-Erweiterungseinschübe	Sechs 2,5-Zoll Hot-swap SAS Festplattenlaufwerkeinschübe	Keine Zusatzoptionen
Festplatte	Zwei 146 GB SAS 2,5" 10K RPM-Festplatten	Keine Zusatzoptionen
RAID-Controller	ServeRAID-MR10i RAID SAS-Adapter, der RAID Level 1 oder 5 verfügbar macht. Einschließlich 256 MB Cache-Modul sowie Batterie für Schreib-Cache	Keine Zusatzoptionen
PCI-Erweiterungssteckplätze	Zwei PCI-Express x16 Gen 2-Steckplätze: - Steckplatz 1 unterstützt eine DUAL NIC-Karte niedrigen Profils (Karten halber Höhe und halber Länge) - Steckplatz 2 unterstützt	Keine Zusatzoptionen

Komponente	Mindestanforderung	Upgrade-Optionen basierend auf Produktanforderungen
	Karten voller Höhe und halber Länge	
Hot-Swap-Lüfter	Sechs	Keine Zusatzoptionen
Netzteil	Ein 675 W, 12 V AC Netzteil	Redundantes 675 W, 12 V AC Netzteil
Video-Controller	Integrierter Matrox G200 (zwei analoge Ports: einer an der Vorderseite, einer hinten, die gleichzeitig angeschlossen werden können) Die maximale Videoauflösung beträgt 1280 x 1024 bei 75 Hz. • SVGA kompatibler Video-Controller • DDR2 250 MHz SDRAM-Video-Memory-Controller • Avocent Digitale Video-Komprimierung • Videospeicher nicht erweiterbar	Keine Zusatzoptionen

Verwandte Themen:

[Einleitung](#) auf Seite 72

Umgebungsvoraussetzungen

Serverstatus	Lufttemperatur	Maximale Höhe	Relative Luftfeuchtigkeit
Server eingeschaltet	10 bis 35° C (50 bis 95° F) in einer Höhe von bis zu 914,4 m (3.000 Fuß)	2.133 m (7.000 Fuß)	8 – 80 %
	10 bis 32° C (50 bis 90° F) in einer Höhe von 914,4 m bis 2.133 m (3.000 bis 7.000 Fuß)		
Server ausgeschaltet	10°C bis 43°C (50,0°F bis 109,4°F)	2.133 m (7.000 Fuß)	8–80 %

Verwandte Themen:

[Einleitung](#) auf Seite 72

Screen Reference

Folgende Änderungen betreffen *Avaya Aura™ Communication Manager Screen Reference*, 03-602878:

AAR und ARS Digit Analysis Table (Ziffernanalysetabelle)

Der * als Platzhalterzeichen ist kein gültiger Eintrag für das Feld **Dialed String** im Bildschirm AAR and ARS Digit Analysis Table.

AAR- und ARS-Ziffernumsetzungstabelle

Der * als Platzhalterzeichen ist kein gültiger Eintrag für das Feld **Matching Pattern** in den Bildschirmen AAR- und ARS-Ziffernumsetzungstabelle.

BCMS/VuStats Service-Level

Auf dem Bildschirm System Parameters Customer-Options (Optional Features) Seite 6, wurde das Feld **BCMS/VuStats Service Level** geändert.

Das Feld **BCMS/VuStats Service Level** erlaubt Ihnen, Sammelgruppen oder Vector Directory Numbers (VDNs) mit einem akzeptablen Service-Level einzurichten. Ein akzeptabler Service-Level definiert die Anzahl der Sekunden, innerhalb derer ein Anruf beantwortet werden muss, damit er als akzeptabel betrachtet werden kann. Der akzeptable Service-Level wird im Bildschirm hunt group eingerichtet, mit dem Feld **Service Level Target (% in sec)**. Das Feld **Acceptable Service Level** wird im Bildschirm VDN verwendet.

Nur-Nebenstellenkennzeichen für Team-Taste auf 96xx H.323-Terminals

Auf dem Bildschirm Feature-Related System Parameters Seite 9, wurde das Feld **Extension only label for Team button on 96xx H.323 terminals** hinzugefügt.

Gültige Einträge	Verwendung
y	Zeigen Sie für 96xx H.323 Telefone die Nebenstellenerweiterung ohne Team-Tastenbeschriftung an. Wenn das Feld Team Btn Display Name auf dem Bildschirm Berechtigungsklasse auf y gesetzt ist, zeigt dieses Feld den Nebenstellennamen ohne Team-Tastenbeschriftung an. 96xx H323 Firmware-Version 2.0 oder darüber ist empfehlenswert, da ein besonders Symbol für Team-Tasten bereitgestellt wird. Das Feld beeinflusst Ihre Beschriftungsanpassung nicht.
n	Zeigen Sie für 96xx H.323 Telefone die Nebenstellenerweiterung mit Team-Tastenbeschriftung an. Wenn das Feld Team Btn Display Name auf dem Bildschirm Berechtigungsklasse auf y gesetzt ist, zeigt dieses Feld den Nebenstellennamen mit Team-Tastenbeschriftung an.

Externes Klingelzeichen für Anrufe mit Amtsleitungen

Auf dem Bildschirm Feature-Related System Parameters Seite 7, wurde das Feld **External Ringing for Calls with Trunks** geändert.

Verwenden Sie dieses Feld, um das Klingelverhalten bei externen Anrufen zu spezifizieren, die von Nebenstellen oder Telefonzentralen weiterverbunden oder zu Konferenzen zusam-

mengelegt werden, oder von einer Telefonzentrale zu einer „on-switch“-Nebenstelle erweitert werden.

Gültiger Eintrag	Verwendung
all-calls	Alle externen Amtsleitungsanrufe, die weiterverbunden oder zu Konferenzen zusammengelegt werden (lokal oder aus der Ferne), erhalten einen externen Klingelton.
local-only	Externe Amtsleitungsanrufe, die weiterverbunden oder zu Konferenzen zusammengelegt werden, erhalten lokal einen externen Klingelton.
none	Für Amtsleitungsanrufe, die weiterverbunden oder zu Konferenzen zusammengelegt werden, gibt es kein externes Klingeln.
remote-only	Externe Amtsleitungsanrufe, die weiterverbunden oder zu Konferenzen zusammengelegt werden, erhalten aus der Ferne einen externen Klingelton. Das ist der Standardwert.

Hunt Group (Sammelgruppe)

Folgende Änderungen sind in Bezug auf den Bildschirm Hunt Group erfolgt:

- Das Feld **Acceptable Service Level (sec)** (Annehmbarer Service-Level (Sek)) wurde vom Bildschirm Hunt Group gelöscht.
- Das Feld **Service Level Target (% in sec)** (Service-Level-Ziel (% in Sek)) und die Feldbeschreibungen für **Interruptible Aux Threshold** wurden geändert.

Interruptible Aux Threshold

Gültiger Eintrag	Verwendung
service-level-target	Gibt an, welcher Schwellenwert ein Ereignis zur Unterbrechung von Sachbearbeitern auslöst, die für eine Fähigkeit unterbrochen werden können. Die Funktion „Unterbrechbare Aux“ wird ausgelöst, wenn der Service-Level in den angegebenen Sekunden unter die verwalteten Prozentaufrufe fällt. Wenn das Ziel beispielsweise 90 % Anrufe in 30 Sekunden ist, wird die Funktion „Interruptible Aux“ ausgelöst, wenn die Messung auf 89 % Anrufe in 30 Sekunden fällt.
none	„Interruptible Aux“ ist für diese Sammelgruppe nicht aktiv.

Service-Level-Ziel (% in Sek)

Wird angezeigt, wenn die Felder **ACD** und **Measured** nicht leer sind, und wenn einer oder mehrere der folgenden Funktionen aktiv sind:

- **BCMS/VuStats Service Level**, das Feld auf dem Bildschirm System Parameters Customer-Options ist aktiv und das Feld **Measured** ist eingestellt auf: Internal oder both. Das Service-Level-Ziel in Sekunden wird als akzeptabler Level für die Berichterstattung des Prozentsatzes der beantworteten Anrufe innerhalb einer angegebenen Zeit verwendet. Der Prozentsatz kann auf den Standard 80 % eingerichtet sein.
- Business Advocate auf dem Bildschirm System Parameters Customer-Options ist aktiv. Service-Level-Ziel in Sekunden wird verwendet, für die Service-Level-Zielvorgabe: Business Advocate Service Level Supervisor. Dieses Service-Level-Ziel kann auch für dynamische Anpassung des Prozentsatzes verwendet werden, wenn das Feld **Dynamic Threshold Adjustment** auf dem Bildschirm Hunt Group y ist und für die dynamische Prozentsatzanpassung, wenn das Feld **Group Type** im Bildschirm Hunt Group ausgefüllt ist und das Feld **Dynamic Percent Adjustment** auf dem Bildschirm Hunt Group auf y steht.
- **Service Level Target** wird angezeigt, wenn das Feld **Group Type** auf dem Bildschirm Hunt Group auf slm steht, und auf dem Bildschirm System Parameters Customer-Options der Service-Level-Maximizer aktiv ist, und die Kundenoptionslizenz Business Advocate nicht aktiv ist. In diesem Fall wird die Einstellung auch als Service-Level-Ziel verwendet, um SLM auszulösen.
- **Interruptible Aux Threshold**, das Feld im Bildschirm Hunt Group, wird auf service-level-target gesetzt. Die Funktion "Interrupt Aux" wird ausgelöst, wenn der Service-Level unter die verwalteten Prozent Anrufe innerhalb der angegebenen Zeit fällt.

Gültiger Eintrag	Verwendung
1 bis 99 (Prozentsatz)	Die Prozentsatzkomponente für Service-Level-Ziel. Der Standardwert ist 80 %.
1 bis 9999 (Zeit in Sekunden)	Die Zeitkomponente für Service-Level-Ziel. Der Standardwert ist 20 Sekunden.

Ankommende Dialog-Prüfschleifen

Anzeige auf dem Bildschirm Signaling Group (Signalisierungsgruppe) wenn das Feld **Group Type** sip ist.

Gültige Einträge	Verwendung
Zulassen	Communication Manager-Software verbindet den Anruf und ermöglicht den SIP-Amtsleitungen, in der Schleifenverbindung zu bleiben. Wenn die von der SIP-Signalisierungsgruppe kontrollierte Amtsleitungsgruppe für IGAR-Anrufe verwendet wird, empfiehlt Avaya den Wert auf allow zu setzen.
eliminate	Communication Manager-Software verbindet den Anruf und löscht die SIP-Amtsleitungen aus der Schleifenverbindung. Voreinstellung ist eliminate.

ISDN Numbering Umwandlung der Calling Party Number (CPN - Rufnummer des Anrufers) für Tandemverbindungen



Hinweis:

Der Bildschirm „Umwandlung der Calling Party Number“ (CPN - Rufnummer des Anrufers) für Tandemverbindungen aktualisiert die Rufnummer des Anrufers in einer NCA-TSC SETUP-Nachricht nicht. Solche Aktualisierungen erfolgen in einer QSIG-Nachrichtenanzeige von einer Voice Mail-Ergänzung.

Standortparameter

Off-PBX Feature Name Extension Set (Funktionsnamenserweiterungen)

Gültiger Eintrag	Verwendung
bis zu zwei Ziffern (0 bis 9) — 1 bis 10 für die mittlere Konfiguration und 1 bis 99 für die große Konfiguration	Der Satz Funktionsnamenserweiterungen (FNE), der für Standort-basierte Anrufverteilung verwendet werden soll.
leer	Steht das Feld auf leer wird der FNE-Standardsatz verwendet. Der Standard ist leer.

Long Distance Access Code

Gültiger Eintrag	Verwendung
bis zu 5 Ziffern (0 bis 9)	Die Vorwahl für Ferngespräche, die das System der Telefonnummer voranstellen soll.
leer	Wenn Sie die Vorwahl nicht verwalten, dann lassen Sie dieses Feld leer. Der Standard ist leer.

off-pbx-telephone station-mapping

Auf dem Bildschirm Off-PBX Telephone Station-Mapping Seite 2 wurde das Feld **Location** verändert.

Standort

Gültige Einträge	Verwendung
1 bis 50 für mittelgroße Konfiguration und 1 bis 250 für große Konfiguration	Richten Sie den Wert Location (Standort) ein, für jede OPS, PBFMC, SPFMC oder PVFMC Anwendung, die Sie auf Seite 1 verwaltet haben. Sie können den Wert Location auf dem Bildschirm Locations finden (<i>Standorte ändern</i>). • Für ein DCP-Tischgerät geben Sie den Standort des Mediengateways ein. • Für ein IP-Tischgerät geben Sie den Standort der Netzwerkregion ein, die zu dem Tischgerät gehört. • Ist das Feld leer, wird der Standort der Amtsleitung für die abgehenden Anrufe von Off-PBX-Endpunkten verwendet, und der Standort der Nebenstelle wird für die ankommenden Anrufe an Off-PBX-Endpunkten verwendet.
leer	Der Standard für dieses Feld ist leer.

Timer der Trennung von abgehenden Amtsverbindungen (Minuten)

Das Feld **Outgoing Trunk Disconnect Timer (minutes)** (Timer der Trennung von abgehenden Amtsverbindungen (Minuten)) wurden von der Seite 2 des Bildschirms **Class of Restriction (COR)** (Berechtigungsklasse) auf Seite 3 des COR-Bildschirms verschoben.

Refresh Terminal Parameters Access Code

Auf dem Bildschirm Feature Access Code (FAC) (Zugriffscod für Leistungsmerkmale), Seite 3, wurde das Feld **Refresh Terminal Parameters Access Code** geändert.

Feature Access Code (FAC) wird verwendet, um einen der Terminalparameter eines Telefons zu aktualisieren, die die herunterladbaren Parameter unterstützen. Immer wenn Sie ein DCP-Telefon installieren oder ersetzen, müssen Sie den **Refresh Terminal Parameters Access Code** verwenden, um sicherzugehen, dass alle Terminalparameter (einschließlich Tastenbeschriftungen) an das Telefon gesendet werden.

Gemeinsam genutzte UUI-Funktionsprioritäten

ASAI

Benutzerinformation von Zusatzsystem-/Switch-Anwendungsschnittstellen (ASAI). Die Priorität kann im Bereich von 1 bis 7 gesetzt werden (1 ist die höchste) oder leer gelassen werden. Standardpriorität ist 1. Wenn das Feld leer ist, wird die Information nicht weitergeleitet.

Erfasste Ziffern

Vom Anrufer erfasste Ziffern (nicht vorgewählte Ziffern ausgenommen). Die Priorität kann im Bereich von 1 bis 7 gesetzt werden (1 ist die höchste) oder leer gelassen werden. Standardpriorität ist 5. Wenn das Feld leer ist, wird die Information nicht weitergeleitet.

Gehaltener Anruf UCID

Der eindeutige Tag für den letzten Anruf, der vom Sachbearbeiter der automatischen Anrufverteilung (ACD) gehalten und an ein anderes System verteilt wurde. Die Universal Call ID (UCID) kann verwendet werden, um den Original- oder übergeordneten Anruf zu identifizieren, der eine Konferenz sein kann oder eine Umleitung an ein anderes System. Das Element ist erforderlich für die Rufverfolgung mit Avaya IQ Version 5.0 und darüber. Die in diesem

Element enthaltene UCID mit Standardpriorität 2 ist die Markierung für diesen neuen Anruf, den der Sachbearbeiter platziert, während der Originalanruf gehalten wird.

Die Priorität kann im Bereich von 1 bis 7 gesetzt werden (1 ist die höchste) oder leer gelassen werden. Standardpriorität ist 7. Wenn das Feld leer ist, wird die Information nicht weitergeleitet.

In-VDN Time

Sekunden, die der Anruf in der Vektorverarbeitung verbracht hat. Die Priorität kann im Bereich von 1 bis 7 gesetzt werden (1 ist die höchste) oder leer gelassen werden. Standardpriorität ist 3. Wenn das Feld leer ist, wird die Information nicht weitergeleitet.

Sonstige LAI-Information

Beinhaltet den Zeitstempel, wann der Anruf in die aktuelle Warteschlange eingegangen ist, die Priorität des Anrufes in der aktuellen Warteschlange und den Überlauftyp. Die Priorität kann im Bereich von 1 bis 7 gesetzt werden (1 ist die höchste) oder leer gelassen werden. Standardpriorität ist 6. Wenn das Feld leer ist, wird die Information nicht weitergeleitet.

Universal Call ID

Eine eindeutige Markierung, die den Anruf kennzeichnet, für den die Nachricht gesendet wurde, und andere Informationen, die in der User-User-Information (UUI) enthalten sind und für den Anruf gelten. Die Priorität kann im Bereich von 1 bis 7 gesetzt werden (1 ist die höchste) oder leer gelassen werden. Standardpriorität ist 2. Wenn das Feld leer ist, wird die Information nicht weitergeleitet.

VDN-Name

Name der aktiven VDN (auch LAI DNIS genannt). Die Priorität kann im Bereich von 1 bis 7 gesetzt werden (1 ist die höchste) oder leer gelassen werden. Standardpriorität ist 4. Wenn das Feld leer ist, wird die Information nicht weitergeleitet.

Station (Nebenstelle)

Survivable COR

Dieses Feld wird vom PIM-Modul des Integrated Management verwendet, damit erfolgreiche Abfragen der Communication Manager-Administrationstabellen erfolgen und die Dienstklasseninformation erhalten wird. PIM-Modul baut eine verwaltete Datenbank auf, um Standard Local Survivability (SLS) auf den H.248-Gateways zu holen. Dieses Feld ist für alle analogen und IP-Nebenstellentypen. Verwenden Sie dieses Feld, um Berechtigungsstufen für Nebenstellen einzurichten, die in Verbindung mit dem ausfallsicheren Rufnummernplan verwendet werden, um bestimmte Benutzer auf bestimmte Anruftypen zu beschränken. Die Berechtigungsstufen werden in der Reihenfolge stärkste Beschränkung bis schwächste Beschränkung aufgelistet. Jeder Level übernimmt die Anrufmöglichkeit derjenigen darüber.

Gültige Einträge	Verwendung
Notfall	Diese Nebenstelle kann nur für Notfallanrufe verwendet werden, diese sind klar definiert.
Intern	Diese Nebenstelle kann nur intern vermittelte Anrufe tätigen. Das ist der Standard.
Lokal	Diese Nebenstelle kann nur Anrufe tätigen, die als locl, op, svc oder hnpa definiert wurden, und zwar in den Survivable Gateway Call Controller's routing tables
Anrufsperr für Ferngespräche	An dieser Nebenstelle können nationale Ferngespräche geführt werden, die in den Survivable Gateway Call Controller's routing tables als fnpa oder natl definiert sind.
Ohne Beschränkung	An dieser Nebenstelle kann ein Anruf an jede beliebige Nummer erfolgen, die in Survivable Gateway Call Controller's routing tables definiert ist. Die Zeichenfolgen, die mit Ablehnen markiert sind, sind diesen Benutzern auch versagt.

Survivable GK Node Name

Das Feld wird von Communication Manager verwendet, um das Vorhandensein anderer H.323 Gatekeepers zu kennzeichnen (befinden sich in Gateway Produkten), die ausfallsichere Anruf Funktionen bieten. Beispielsweise die MultiTech MVPxxx-AV H.323 Gateway-Familie und die SLS-Funktion in H.248-Gateways. Wenn in dieses Feld ein gültiger IP-Knotenname eingegeben wird, fügt Communication Manager die IP-Adresse des Gateways am Ende der „Ausweich-Gatekeeper-Liste“ für diese IP-Netzwerkregion hinzu. Da die H.323 IP-Nebenstelle sich bei Communication Manager registriert, wird diese Liste in die Registrierungs-Bestätigungsnachricht gesendet. Das ermöglicht der IP-Nebenstelle, die IP-Adresse des Survivab-

le Gatekeeper als Not-Anruf-Controller für die Registrierung zu verwenden. Das Feld wird angezeigt, wenn das Feld **TYPE** eine H.323-Nebenstelle ist (46xx oder 96xx Modelle). Wenn es keine externen Gatekeeper-Knoten in einem Kunden-Netzwerk gibt, muss das Feld leer bleiben.

Gültige Einträge	Verwendung
gültiger IP-Knotenname oder leer	Geben Sie einen gültigen IP-Knotennamen ein wie er auf dem Bildschirm IP Node Names verwaltet wird, damit die Nebenstelle als ein IP-Telefon registriert wird, das zu einem H.323-Gateway gehört und fähig ist, einen Gatekeeper in ausfallsicherem Modus zu unterstützen. Der Standard ist leer.

Survivable Trunk Dest

Dieses Feld wird vom PIM-Modul des Integrated Management verwendet, damit erfolgreiche Abfragen der Communication Manager-Administrationstabellen erfolgen und die Dienstklasseninformation erhalten wird. PIM-Modul baut eine verwaltete Datenbank auf, um Standard Local Survivability (SLS) auf den H.248-Gateways zu holen. Dieses Feld ist für alle analogen und IP-Nebenstellentypen. Verwenden Sie dieses Feld, um bestimmte Telefone zu kennzeichnen, die keine Erlaubnis haben, ankommenden Amtsverbindungen zu empfangen, wenn das Media Gateway im ausfallsicheren Modus ist.

Gültige Einträge	Verwendung
y	Geben Sie <i>y</i> ein, um Nebenstellen zu erlauben, Ziel ankommender Amtsleitungen zu sein, wenn das Media Gateway im ausfallsicheren Modus läuft. Das ist der Standard.
n	Geben Sie <i>n</i> ein, um zu verhindern, dass diese Nebenstelle im ausfallsicheren Modus ankommende Amtsleitungen empfängt.

Survivable ARS Analysis Table (Ausfallsichere ARS-Ziffernanalysetabelle)

Der Bildschirm Survivable ARS Analysis Table ist kein gültiger Bildschirm und wird aus *Avaya Aura™ Communication Manager Screen Reference* entfernt..

Trunk Group

Analog Loss Group:

Das Feld legt fest, welche verwaltete 2-Parteienzeile im Dämpfungsplan für dieses Amtsleitungsbündel zutrifft, wenn der Anruf über einen analogen Signalisierungs-Port in das Amtsleitungsbündel übertragen wird.

Gültiger Eintrag	Verwendung
1–17	Zeigt den Index in den Dämpfungs- und Tonplan. Wenn Sie das Feld Analog Loss Group anders verwalten als zwischen 6-10 oder 15-17 Einträgen, erhalten Sie eine Warnmeldung die angibt, dass die Loss Group möglicherweise für dieses Amtsleitungsbündel nicht angemessen ist.

Digital Loss Group:

Das Feld legt fest, welche verwaltete 2-Parteienzeile im Dämpfungsplan für dieses Amtsleitungsbündel zutrifft, wenn der Anruf über einen digitalen Signalisierungs-Port in das Amtsleitungsbündel übertragen wird.

Gültiger Eintrag	Verwendung
1–19	Zeigt den Index in den Dämpfungs- und Tonplan. Wenn Sie das Feld Digital Loss Group anders verwalten als zwischen 11-15 oder 18 Einträgen, erhalten Sie eine Warnmeldung die angibt, dass die Loss Group möglicherweise für dieses Amtsleitungsbündel nicht angemessen ist.

Uniform Dial Plan Table (Rufnummernplan-Tabelle)

Das Feld **Acceptable Service Level (sec)** ist kein gültiges Feld im Bildschirm Uniform Dial Plan Table und wird aus *Avaya Aura™ Communication Manager Screen Reference* entfernt..

Verwenden Sie „Trunk COR“ für die Unterbrechung der ausgehenden Amtsleitung

Das Feld **Use Trunk COR for Outgoing Trunk Disconnect** (Verwenden Sie „Trunk COR“ für die Unterbrechung der ausgehenden Amtsleitung) wurde umbenannt in **Use Trunk COR for Outgoing Trunk Disconnect/Alert** (Verwenden Sie „Trunk COR“ für die Unterbrechung der ausgehenden Amtsleitung/Meldung) auf der Seite 6 des Bildschirms „Feature-Related System Parameters“ (Funktionsbezogene Systemparameter).

„VDN Override for ISDN Trunk ASAI Messages“ (VDN-Umgehung für ASAI-Nachrichten über ISDN-Amtsleitungen).

Das Feld **VDN Override for ISDN Trunk ASAI Messages** wurde umbenannt in **VDN Override for ASAI Messages** auf Seite 2 des Bildschirms „Vector Directory Number“ und auch die Feldbeschreibung wurde geändert.

VDN-Umgehung für ASAI-Nachrichten

Wenn **Meet-me Conferencing** nist, wird ein Asterisk (*) neben dem Feldnamen angezeigt, das angibt, dass das Feld VDN-Umgehungsregeln folgt, wenn das System die „aktive“ VDN für einen Anruf ändert. Das Feld ist nur verfügbar, wenn folgende Bedingungen in der Communication Manager-Lizenzdatei eingerichtet sind:

- Auf dem Bildschirm System Parameters Customer-Options (Optional Features) ist das Feld **ASAI Link Core Capabilities** auf y.
- Auf dem Bildschirm System Parameters Customer-Options (Optional Features) ist das Feld **G3 Version** auf V10 oder darüber gesetzt.

Zusätzlich können Sie dieses Feld nur auf ISDN Trunk oder all einrichten, wenn das Feld **Allow VDN Override** aus diesem VDN-Bildschirm ebenfalls auf y steht. Wenn **Meet-me Conferencing** nist, wird ein Asterisk (*) neben dem Feldnamen angezeigt, das angibt, dass das Feld VDN-Umgehungsregeln folgt, wenn das System die „aktive“ VDN für einen Anruf ändert. Die „aktive“ VDN ist die VDN, die den Anruf empfängt und wird zu einem an VDN weitergeleiteten geändert, wenn in der VDN-Anrufweiterleitung das Feld "Allow VDN Override" auf y steht.

Gültiger Eintrag	Verwendung
n	Die "Information "Angerufene Nummer"" gesendet für "Call Offered", "Alerting", "Queued" und "Connect" ASAI-Ereignis-Benachrichtigung und Zusatz-Anforderungsnachricht sind immer die angerufene VDN-Nebenstelle in der Called Number IE, die in der ankommenden ISDN SETUP-Nachricht oder der lokalen An-

Gültiger Eintrag	Verwendung
	rufnummer gesendet wird, und ändern sich nicht nach Weiterleitung an die angerufene VDN bzw. nachfolgende VDNs.
ISDN-Amtsleitung	Wenn eine ankommender ISDN-Amtsleitungsanruf an diese VDN weitergeleitet wird, wird die "Information "Angerufene Nummer"" an das ASAI-Ereignis gesendet und "Adjunct Route Request" ASAI-Nachrichten ist die "aktive VDN" -Nebenstelle die dem Anruf zugewiesen wird, basierend auf den VDN-Umgehungsregeln. Diese Option trifft nicht für lokale/interne Anrufe zur Verfügung.
all	Gibt der Funktion VDN-Umgehung für ASAI-Nachrichten die oben genannten Optionen, damit die aktive VDN für die angerufene Nummer für alle Anruftypen an VDN verwendet wird, einschließlich lokaler/interner Anrufe sowie externe ankommende ISDN-Amtsleitungsanrufe.

Index

14xx digitale Telefone	
Firmware-Download-Anforderungen	8

A

AAR und ARS Digit Analysis Table (Ziffernanalysetabelle)	82
AAR- und ARS-Ziffernumsetzungstabelle	82
Administration des Avaya G450-Mediengateways	
DHCP-Server CLI-Konfiguration	73
Administration für das Avaya G450 Media Gateway	73
aktiv	17
Aktivieren der Medienverschlüsselung für das Gateway	55
Aktivieren von Alarm für SAL	70
Aktivierung von Prozessor-Ethernet	69
Aktualisieren von Communication Manager R5.1.x auf CM Messaging R5.2.1 auf einem S85XX Server	55
Aktualisieren von Communication Manager von R5.1 auf R5.2.1	56
Amtsleitungsbündel	
Analog Loss Group	92
Digital Loss Group	92
Ändern der Berechtigungsklasse	62
Ändern der Systemparameter – Weiterleitung	62
Ändern von Kundenoptionen, um Medienverschlüsselung zu ermöglichen	53
Ändern von Signalisierungsgruppe, um Medienverschlüsselung zu ermöglichen	53
Änderungen am Administrator Guide	73
Anforderungen an elektrische Leistungsaufnahme	78
Ankommende Dialog-Prüfschleifen	85
Anmeldung beim CM-Server mit PuTTY	52
ARP-Spoofing-Schutz	43
Avaya Site Administration	74
Avaya-Mediengateway, Änderungen	
ARP-Spoofing-Schutz	43
Avaya-Mediengateways - Veränderungen	
MP20 - erhöhte Kapazität	36
Avaya-Mediengateways, Änderungen	35–40, 42–44, 46
G450 - erhöhte Kapazität	35
ip arp inspection	43
Plattform-Hauptplatine anzeigen	39
power-down reset	46
Protokollerweiterungen	44
reset power-down	46

show voip-dsp	36, 40
show voip-parameters	35, 37, 42
System anzeigen	38

B

BCMS/VuStats Service-Level	83
Beenden von OCM nach Antwort (ms)	31
Bei Aktualisierungen unterstützte Server (nach Version)	12
Berechtigungsklasse	
Timer der Trennung von abgehenden Amtsverbindungen (Minuten)	88

C

Call Center 5.2.1 Erweiterungen	7
---------------------------------------	-------------------

D

DHCP-Server CLI-Konfiguration	73
Direktanschluss	19
DNY_CLASS_NO_CAP	33
Dokumentations- und Verfahrensaktualisierungen	73

E

Einrichten der One-X Server-Integration	74
Einrichten des IP-Codecsatzes	54
Einrichten des SRTP-Typs auf der CM Messaging-Verwaltungswebschnittstelle	54
Ende OCM-Intercept-Erweiterung	31
Erhöhen und Verringern der Verfügbarkeit des S8800 Servers	64
Erstellen eines Benutzer-basierten Profils	59
Externes Klingelzeichen für Anrufe mit Amtsleitungen ...	83

F

Feature-Related System Parameters (Funktionsbezogene Systemparameter)	
Externes Klingelzeichen für Anrufe mit Amtsleitungen	83
Nur-Nebenstellenkennzeichen für Team-Taste auf 96xx H.323-Terminals	83
Festplatte	
Technische Daten	80

Feuchtigkeitsvoraussetzungen	82
Funktionen der 14xx Digitaltelefone	71
Funktionsbeschreibung und Implementierungänderungen	74
Funktionsbezogene Systemparameter	
Verwenden von „Trunk COR“ für Unterbrechung ausgehender Amtsleitung	93

G

G450 - erhöhte Kapazität	35
Gemeinsam genutzte UUI-Funktionsprioritäten	
ASAI	88
Erfasste Ziffern	88
Gehaltener Anruf UCID	88
In-VDN Time	89
Sonstige LAI-Information	89
Universal Call ID	89
VDN-Name	89

H

Hardware	71
Hardwarebeschreibung und -übersicht - Änderungen ...	75
Hinweise, rechtliche	2
Höhenvoraussetzungen	82

I

Installation des Avaya S8800 Servers für SES	49
Installation von CM Messaging R5.2.1	56
Installation von Communication Manager	63
Installation von Communication Manager auf einem S8800	63
Installation von Communication Manager Messaging	51
Installation von Communication Manager Messaging auf einem S8800 Server	51
Interaktionen für Leitungstastenkopie	
Notrufe	75
Interaktionen für Whisper Paging	
Aufschaltfunktion	75
Interruptible Aux Threshold	84
ip arp inspection	43

K

Kadenzklassifizierung nach Antwort	32
Kernel	13
Konfiguration von CM und Serverstatusparametern	66
Konfigurieren von SAL-Gateway	70

L

Lärmemissionen	78
LDAP-Prozesse	57
LDAP-Überblick	57
Loginprofil - Überblick	58
Long Distance Access Code	87
Lüfter	
Technische Daten	80

M

Manuelle Konfiguration des CM-Servers	64
Medienlaufwerk	
Technische Daten	80
memory	
Technische Daten	80
Migration von S8500 und S8510 Servern zum S8800 Server	49
Mikroprozessor	
Technische Daten	80
Modi der Nicht-Kadenz-Anrufklassifizierung und End- OCM-Timer	
Anrufbearbeitungsszenarien	23
MP20 - erhöhte Kapazität	36

N

Netzteil	
Technische Daten	80
Neue Serverunterstützung für Communication Manager Messaging	51
Neustarten der Messaging-Anwendung	54
Nicht-Kadenz Ruftonklassifizierungsmodi und End- OCM-Timer	
Bedingungen	27
detaillierte Beschreibung	22
Einrichten der Ansagennebenstelle	26
Einrichten von End-OCM-Timer	26
Einrichten von Nicht-Kadenz Ruftonklassifizierungs- modi	26
Firmware-Anforderungen	23
Interaktionen	28
Verwaltungsbildschirme	26
Nur-Nebenstellenkennzeichen für Team-Taste auf 96xx H.323-Terminals	83

O

Off-PBX Feature Name Extension Set (Funktionsna- menserweiterungen)	86
--	--------------------

off-pbx-telephone station-mapping	87
Standort	87

P

PCI-Steckplatz	
Technische Daten	80
power-down reset	46
Protokollerweiterungen	44
Prozessor-Ethernet-IP-Schnittstelle	68

R

RAID-Controller	
Technische Daten	80
rechtliche Hinweise	2
Refresh Terminal Parameters Access Code	88
reset power-down	46
RFC 3389 Rauschsignal	9

S

S8800 Einleitung	72
S8800 Ethernet-Portzuordnungen	66
Sammelgruppe	
Annehmbarer Service-Level (Sek)	84
Service-Level-Ziel (% in Sek)	84 , 85
Unterbrechbare AUX-Schwellenwert	84
Screen Reference, Änderungen	82
Secure Real-Time Transport Protocol	52
Server	
Gewicht	78
Komponenten	80
Maße	78
Rückansicht	77
Technische Daten	78
Server-Migrationspfad	9
Service-Level-Ziel (% in Sek)	85
SES Mixed-mode Trusted Host Interface	49
SES-Änderungen	49
show platform mainboard	39
show voip-dsp	36 , 40
show voip-parameters	35 , 37 , 42
Sichern und Wiederherstellen von CM Messaging-Daten	60
Sichern von CM-Messaging-Daten	60
Signalisierungsgruppe	
Ankommende Dialog-Prüfschleifen	85
RFC 3389 Rauschsignal	9
Softwaredoppelung	67
Spezialanwendung, Aktivierungsprozess	33
Standort	87
Standortparameter	
Beenden von OCM nach Antwort (ms)	31

Ende OCM-Intercept-Erweiterung	31
Long Distance Access Code	87
Off-PBX Feature Name Extension Set (Funktionsnamenserweiterungen)	86
Statusüberprüfung der LDAP-Prozesse	58
Survivable ARS Analysis Table (Ausfallsichere ARS-Ziffernanalysetabelle)	91
System anzeigen	38
System Management-Schnittstelle	14
Systemparameter OCM-Ruftonklassifizierung	
Kadenzklassifizierung nach Antwort	32

T

Taste für sofortiges Weiterleiten	74
Temperaturvoraussetzungen	82
Tests	17
Timer der Trennung von abgehenden Amtsverbindungen (Minuten)	88
TN791Baugruppe	75

U

Überwachung von Communication Manager und Serverstatus	65
Umgebungsbedingungen	82
Uniform Dial Plan Table (Rufnummernplan-Tabelle)	92
Unterstützung der Avaya 14xx Digitaltelefone	7
update_activate	21
update_deactivate	22
update_show	21

V

VDN-Umgehung für ASAI-Nachrichten	93
Verbinden zu LDAP	57
Verbindung zum Server mit SAL	70
Verwalten von Aktualisierungen	17
Verwaltung von Nicht-Kadenz Ruftonklassifizierungsmodi und End-OCM-Timer	25
Video-Controller	
Technische Daten	80

W

Wärmeleistung	78
---------------------	--------------------

Z

Zugriff auf den CM Server	52
Zugriff auf die Webseite „Configure Health Monitor“ (Statusüberwachung konfigurieren)	65

Index

Zugriff auf Messaging für alle Nicht-SRTP kompatiblen Endpunkte zulassen	55	Zuweisen der IP-Adresse für Prozessor-Ethernet auf der System Management-Schnittstelle	69
Zugriffscode für Leistungsmerkmale (FAC) Refresh Terminal Parameters Access Code	88	Zuweisen der IP-Adresse zu Prozessor-Ethernet	68
		Zuweisen eines Profils zu einem Benutzer	59