

CA IT Client Manager

Data Transport Service- Administrationshandbuch

Version 12.8



Diese Dokumentation, die eingebettete Hilfesysteme und elektronisch verteilte Materialien beinhaltet (im Folgenden als "Dokumentation" bezeichnet), dient ausschließlich zu Informationszwecken des Nutzers und kann von CA jederzeit geändert oder zurückgenommen werden. Diese Dokumentation ist Eigentum von CA und darf ohne vorherige schriftliche Genehmigung von CA weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden.

Der Benutzer, der über eine Lizenz für das bzw. die in dieser Dokumentation berücksichtigten Software-Produkt(e) verfügt, ist berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen innerbetrieblichen Gebrauch im Zusammenhang mit der betreffenden Software auszudrucken, vorausgesetzt, dass jedes Exemplar diesen Urheberrechtsvermerk und sonstige Hinweise von CA enthält.

Dieses Recht zum Drucken oder anderweitigen Anfertigen einer Kopie der Dokumentation beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenz. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Lizenznehmer gegenüber CA schriftlich, dass alle Kopien oder Teilkopien der Dokumentation an CA zurückgegeben oder vernichtet worden sind.

SOWEIT NACH ANWENDBAREM RECHT ERLAUBT, STELLT CA DIESE DOKUMENTATION IM VORLIEGENDEN ZUSTAND OHNE JEGICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN INSBESONDERE STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET CA GEGENÜBER IHNEN ODER DRITTEN GEGENÜBER FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER NUTZUNG DIESER DOKUMENTATION ENTSTEHEN; DAZU GEHÖREN INSBESONDERE ENTGANGENE GEWINNE, VERLORENGEGANGENE INVESTITIONEN, BETRIEBSUNTERBRECHUNG, VERLUST VON GOODWILL ODER DATENVERLUST, SELBST WENN CA ÜBER DIE MÖGLICHKEIT DIESES VERLUSTES ODER SCHADENS INFORMIERT WURDE.

Die Verwendung aller in der Dokumentation aufgeführten Software-Produkte unterliegt den entsprechenden Lizenzvereinbarungen, und diese werden durch die Bedingungen dieser rechtlichen Hinweise in keiner Weise verändert.

Diese Dokumentation wurde von CA hergestellt.

Zur Verfügung gestellt mit „Restricted Rights“ (eingeschränkten Rechten) geliefert. Die Verwendung, Duplizierung oder Veröffentlichung durch die US-Regierung unterliegt den in FAR, Absätze 12.212, 52.227-14 und 52.227-19(c)(1) bis (2) und DFARS, Absatz 252.227-7014(b)(3) festgelegten Einschränkungen, soweit anwendbar, oder deren Nachfolgebestimmungen.

Copyright © 2013 CA. Alle Rechte vorbehalten. Alle Markenzeichen, Markennamen, Dienstleistungsmarken und Logos, auf die hier verwiesen wird, sind Eigentum der jeweiligen Unternehmen.

CA Technologies-Produktreferenzen

Diese Dokumentation bezieht sich auf die folgenden CA-Produkte:

- CA Advantage® Data Transport® (CA Data Transport)
- CA Asset Intelligence
- CA Asset Portfolio Management (CA APM)
- CA Common Services™
- CA Desktop Migration Manager (CA DMM)
- CA Embedded Entitlements Manager (CA EEM)
- CA Network and Systems Management (CA NSM)
- CA Patch Manager
- CA Process Automation
- CA Business Intelligence
- CA Service Desk Manager
- CA WorldView™
- CleverPath™ Reporter

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter <http://www.ca.com/worldwide>. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Inhalt

Kapitel 1: Willkommen bei Data Transport Service 9

Vorteile und Funktionen	10
Netzwerk-Administration	11
Befehlszeilenschnittstelle.....	12
Self Discovery	14
Dynamische Container und dynamisches Routing	14
Fehlermeldungen	15
Unterstützung für das Übertragen großer Dateien.....	15
PIF-Installationspakete für UNIX	15
Integration von DTS und CA Common Services.....	15
WorldView	17
Enterprise-Management	19
Datenübertragungen	20
Alternatives Routing.....	20
Diskrete Übertragungen.....	21
Maximale Anzahl von Übertragungen pro Job in einer Fanout-, Broadcast- oder Multicast-Übertragung	21
Konfiguration des Staging-Verzeichnisses.....	21
Auditing	22
Handhabung von DHCP- und Modemverbindungen.....	22
HTTP-Protokollunterstützung	23
Protokollauswahl	23
Externe Protokolle	23

Kapitel 2: Architektur 25

Überblick	25
DTS-Manager	26
Network Object Server.....	26
Transfer Object Server (TOS).....	29
Schedule Object Server (SOS)	31
UNIX-Manager.....	31
DTS-Agent.....	31
Initiator	31
Responder	32
Sender- und Empfängeraufgaben	32
Filter	35
DTS-Client-API	37

DTS-Browser	38
DTS-Sicherheit	38

Kapitel 3: Implementierung **39**

Standardkonfiguration	39
Andere mögliche Konfigurationen	40
Implementierungsmodell	40
Objektmodell	43
Referenzverknüpfungen zwischen verschiedenen Objekten	45
DTS-Szenario	46
Datenübertragungsprobleme	47
Die Datenübertragungslösung	48
Lösen des Problems	49
Erstellen eines Netzwerkmodells	50
Erstellen von Übertragungsobjekten	53

Kapitel 4: Konfigurieren des Data Transport Service **55**

Anzeigen der Konfigurationsrichtlinien	55
Ändern der Konfigurationsrichtlinien	56

Kapitel 5: Anpassen des Data Transport Service **57**

Erstellen einer Netzwerktopologie	57
Ändern der Audit-Ebenen	59
Aktivieren/Deaktivieren von Agent-Auditing	60
Aktivieren/Deaktivieren von TOS-Auditing	60
Aktivieren/Deaktivieren von NOS-Auditing	61
Aktivieren/Deaktivieren von SOS-Auditing	62
Anpassen von Audit-Meldungen	62
Audit-Protokolldateien	63
Audit-Token	63
Anpassen von Audit-Tokens	64
Makros	66
Anpassen von Makros	66

Kapitel 6: Optimieren einer Datenübertragung **69**

Phase 1: Netzwerkruutenanalyse	69
Phase 2: Übertragungseigenschaftenauflösung	70
Verknüpfungsobjekteigenschaften	71
Eigenschaften von Computercontainerobjekten	71

Schnittstellenobjekteigenschaften.....	71
Kommunikationseinstellungen	72
Phase 3: Auflösen doppelter Übertragungen.....	73
Phase 4: Auswahl des Übertragungsverfahrens.....	73
Übertragungsressourcennutzung	74
Beziehung zwischen Broadcasts und Verknüpfungs- oder Containereigenschaften	74
Punkt-zu-Punkt-Übertragungen	75
Fanout-Übertragungen	75
Punkt-zu-Viele-Übertragungen	76

Kapitel 7: Übertragungsprotokolle und -verfahren **79**

Protocol Wrapper Interface (PWI)	79
TCP	79
UDP.....	79
IP-Broadcast oder BCAST.....	80
Berechnen einer Broadcast-Adresse.....	80
IP-Multicast oder MCAST	81
Reservierte und registrierte Multicast-Adressen	82
UDP-Betrieb und Einschränkungen	83
Empfehlungen für Multicast-Gruppen	84
Verwenden mehrerer Liefermethoden.....	85
Konfigurieren der Server für die Verwendung von Fanout für kontinentübergreifende Übertragungen	86
Verwenden von Broadcast für lokale Übertragungen	86
Erstellen von Containern und Verknüpfungen für Desktops	87

Kapitel 8: Diagnose und Fehlerbehebung **89**

Erfassungstool für Protokolldateien dsminfo.....	89
CAM-Kommunikation funktioniert nicht.....	90
Multicast-Übertragung fehlgeschlagen (Windows)	90
Multicast-Übertragung fehlgeschlagen (UNIX)	91
Business Process Views-Installation schlägt fehl.....	92
DFÜ-Unterstützung funktioniert nicht	92
Technischer Support	93

Anhang A: Befehle **95**

Befehle "dtacli" und "dtscli".....	95
Befehl "dtscli" – Verwalten von Datenübertragungen.....	95

Anhang B: Unterstützung für externe Filter	99
Terminologieglossar	101

Kapitel 1: Willkommen bei Data Transport Service

Der Data Transport Service ist ein umfassendes Netzwerk, mit dem Sie Daten zuverlässig und effizient über eine Vielzahl von Plattformen und Übertragungsprotokollen übertragen können. Mit DTS haben Sie folgende Möglichkeiten:

- Erstellen, Planen und Auslösen von Datenübertragungen
- Überwachen und Steuern aktiver Datenübertragungen
- Erstellen logischer Rechnergruppen im Netzwerk, um die Datenübertragungen von mehreren Endsystemen effektiver zu verwalten
- Optimieren der Netzwerkleistung mit Hilfe von Übertragungseinstellungen, durch die die Sende- und Empfangsvorgänge bei Datenübertragungen zwischen Computern gesteuert werden
- Remote-Administration des DTS-Netzwerks

Hinweis: Der Begriff Windows bezieht sich auf das Betriebssystem Microsoft Windows, einschließlich Windows XP, Windows Vista, Windows 7, Windows Server 2003 und Windows Server 2008. Sofern nichts anderes angegeben ist, bezieht sich der Begriff Windows auf jedes unterstützte Microsoft Windows-Betriebssystem.

Dieses Kapitel enthält folgende Themen:

[Vorteile und Funktionen](#) (siehe Seite 10)

[Netzwerk-Administration](#) (siehe Seite 11)

[Integration von DTS und CA Common Services](#) (siehe Seite 15)

[Datenübertragungen](#) (siehe Seite 20)

Vorteile und Funktionen

DTS wird mit CA-Client-Lösungen wie CA ITCM geliefert und von diesen verwendet. Die Client-Lösungen ermöglichen eine automatische Installation von DTS unter Verwendung einer vordefinierten Konfiguration. Sie haben jedoch auch die Möglichkeit, die Konfiguration von DTS während des Installationsprozesses an Ihre Anforderungen anzupassen. Die Funktionen von DTS werden erweitert, wenn Sie die CA Common Services-Komponenten (CCS) WorldView und Event Management installieren.

Anleitungen zur Verwendungsweise einer CA-Lösung, die speziell für die Zusammenarbeit mit DTS entwickelt wurde, finden Sie in der Dokumentation und Online-Hilfe der Lösung. Im Allgemeinen beschreibt die Online-Hilfe einer Lösung, wie diese nach der Installation und Konfiguration von DTS auf allen gewünschten Computern im Netzwerk verwendet wird. Selbst wenn DTS bei der Installation der Lösung automatisch installiert wird, müssen Sie DTS möglicherweise auf einigen Computern im Netzwerk konfigurieren. Wenn Sie Verknüpfungen mit Rechnern erstellen möchten, können Sie z. B. die vom Rechner verwendeten Protokolle konfigurieren oder andere rechnerbezogene Eigenschaften festlegen.

Hinweis: Weitere Informationen finden Sie im Abschnitt "Konfigurationsrichtlinie" in der *DSM-Explorer-Hilfe*.

Die Vorteile und Funktionen von DTS lassen sich in die folgenden Kategorien gliedern:

Netzwerk-Administration

Mit Data Transport Service können Datenübertragungen ohne Netzwerkadministration geplant, ausgelöst, überwacht und gesteuert werden. Bei Bedarf können Netzwerkadministratoren jedoch Administrationstasks durchführen, beispielsweise angepasste Netzwerktopologien erstellen und die Netzwerkleistung optimieren.

Integration in CA Common Services

Data Transport Service bietet weitere Funktionen durch die Integration in die CSS-Komponenten WorldView und Event Management.

Hinweis: WorldView wird derzeit ausschließlich auf Windows-Computern mit einer MS-SQL-Datenbank unterstützt. Weitere Informationen zu unterstützten Datenbanken und Betriebsumgebungen finden Sie im *Implementierungshandbuch*.

Datenübertragung

Mit Hilfe des Data Transport Services kann der Administrator Datenübertragungen über verschiedene Plattformen und Übertragungsprotokolle erstellen und auslösen. Übertragungen können unmittelbar aktiviert oder für einen späteren Zeitpunkt geplant werden.

Sie können über unterschiedliche Schnittstellen auf die Vorteile und Funktionen von DTS zugreifen:

- Grafische Benutzeroberfläche für die Netzwerkadministration (Admin-Client-Schnittstelle)
- Grafische Benutzeroberfläche für das Konfigurieren von Richtlinien für DTS-Agenten in CA ITCM
- Programmoberfläche (API) für Client-Anwendung
- Befehlszeilenschnittstelle

Netzwerk-Administration

Netzwerkadministratoren führen Administrationstasks durch wie beispielsweise die Erstellung angepasster Netzwerktopologien und die Optimierung der Netzwerkleistung. Sie können mit DTS Datenübertragungen mit oder ohne Netzwerkadministration planen, einleiten, überwachen und steuern.

Hinweis: Netzwerkadministratoren, die DTS-Netzwerk-Komponenten installieren und verwalten oder die CA-Client-Lösung mit DTS installieren und verwalten, müssen umfassende Kenntnisse zu CSS und den Konventionen des Betriebssystems der Computer haben, auf denen Agenten installiert und verwaltet werden.

Administratoren können die Ergebnisse des DTS-Registrierungsprozesses verwenden, der nach allen DTS-Manager- und Agenten-Komponenten im Netzwerk sucht, um eine bestimmte Netzwerktopologie zu erstellen. Mit dieser Topologie können Sie angepasste Übertragungsrouten im Netzwerk festlegen.

DTS-Administratoren können darüber hinaus Übertragungseinstellungen festlegen, durch die die Sende- und Empfangsvorgänge bei Datenübertragungen zwischen verschiedenen DTS-Computern gesteuert werden. Mit Hilfe dieser Übertragungseinstellungen kann die Netzwerkleistung optimiert werden, da auf diese Weise die maximale Anzahl der zu übertragenden Pakete, die Wartezeit zwischen einzelnen Paketsendungen und die maximale Anzahl der gleichzeitig ausgeführten Prozesse festgelegt wird.

Administratoren können auch die Laufzeitparameter für *Legacy*-Komponenten der Agenten und Manager von Data Transport Service r1, r2 und r3 (NOS, TOS und SOS) per Remote-Zugriff konfigurieren. Sie können alle oben beschriebenen Verwaltungsfunktionen mit CA Common Services konfigurieren. Diese Funktionen können auch über die DTS-Client-API konfiguriert werden.

In CA ITCM werden DTS-Agenten und -Manager über Konfigurationsrichtlinien gesteuert, die mit dem DSM-Explorer eingerichtet werden.

Weitere Informationen:

[Anzeigen der Konfigurationsrichtlinien](#) (siehe Seite 55)

[Ändern der Konfigurationsrichtlinien](#) (siehe Seite 56)

Befehlszeilenschnittstelle

DTS stellt Netzwerkadministratoren eine Befehlszeilenschnittstelle zur Verfügung mit der Übertragungen geplant und ausgelöst oder DTS-Komponenten gestartet und beendet bzw. der Status dieser Komponenten angezeigt werden kann. CA-Lösungen, die mit DTS zusammenarbeiten, stellen eine zusätzliche Befehlszeilenschnittstelle, die Data Transport Service-Befehlszeilenschnittstelle (DTSCLI), zum Auslösen, Überwachen und Steuern von Datenübertragungen über die Befehlszeile bereit.

Weitere Informationen:

[Transfer Object Server \(TOS\)](#) (siehe Seite 29)

dtscli (Befehl)

Mit dem Befehl "dtscli" haben Sie folgende Möglichkeiten:

- Erstellen von Übertragungen, Übertragungsjobs und Übertragungsplänen
- Löschen von Übertragungen, Übertragungsjobs und Übertragungsplänen
- Abfragen des Status von Übertragungen, Übertragungsjobs und Übertragungsplänen
- Hinzufügen, Einfügen und Entfernen von Übertragungen zu, in bzw. aus Übertragungsjobs
- Aktivieren, Zurücksetzen, Abbrechen, Aussetzen und Wiederaufnehmen von Übertragungsjobs
- Einstellen der Priorität eines Übertragungsjobs
- Hinzufügen, Einfügen und Entfernen von Übertragungsjobs zu, in bzw. aus Zeitplänen
- Aktivieren und Deaktivieren von Zeitplänen
- Durchführen von Agent-zu-Agent-Übertragungen
- Durchführen von verwalteten Übertragungen

Darüber hinaus bietet der Befehl "dtscli" Funktionen wie HTTP-Übertragungen (Internet-Downloads), die Erstellung und Bearbeitung von Übertragungsjobs und Zeitplänen sowie die Übernahme von Eingaben aus einer Befehlsdatei.

Hinweis: In CA ITCM wurde "dtacli" durch "dtscli" ersetzt. Obwohl "dtacli" noch vorhanden ist, wird empfohlen, zu "dtscli" zu migrieren.

Weitere Informationen:

[Erstellen von Übertragungsobjekten](#) (siehe Seite 53)

[DTS-Sicherheit](#) (siehe Seite 38)

[Befehle "dtacli" und "dtscli"](#) (siehe Seite 95)

Self Discovery

DTS fügt die DTS-Agenten und -Manager automatisch der Management-Datenbank (MDB) hinzu, sobald diese beim Start eine Benachrichtigung an den TOS senden. Dieser Vorgang wird als *Self Discovery* bezeichnet. Standardmäßig sind alle Agenten und Manager so konfiguriert, dass sie den TOS benachrichtigen, wenn sie starten, beispielsweise nach einem Neustart oder dem ersten Start des Computers. Agenten benachrichtigen den TOS auch bei einer Änderung ihrer Adressen, was häufig bei Roaming-Agenten wie Laptop-Computern oder Agenten, die eine DHCP-Adresse verwenden, auftritt. Der TOS leitet diese Meldung an den NOS weiter.

Wenn der NOS eine Benachrichtigungsmeldung von einem Agenten oder Manager erhält (entweder direkt oder weitergeleitet durch den TOS), überprüft der NOS die MDB, um zu ermitteln, ob der Agent oder Manager bereits in dem Repository vorhanden ist. Ist dies nicht der Fall, fügt der NOS den Agenten oder Manager dem Repository hinzu.

Self Discovery ist in CA ITCM standardmäßig deaktiviert. Um diesen Prozess zu aktivieren, ändern Sie den Wert der Konfigurationsrichtlinie für Self Discovery in der Richtliniengruppe "Network Object Server" (NOS).

Weitere Informationen:

[Ändern der Konfigurationsrichtlinien](#) (siehe Seite 56)

Dynamische Container und dynamisches Routing

Mit dynamischen Containern wird Routing von Computern in einer dynamischen Umgebung ermöglicht. Dynamische Container sind Data Transport-Klassen, die Sie in WorldView als Teil der MDB erstellen und verwalten. Bei der Erstellung eines dynamischen Containers geben Sie einen Adressbereich oder ein Subnetz an. Alle Agenten, deren IP-Adressen sich in diesem Bereich befinden, werden Mitglieder des dynamischen Containers. Durch die Erstellung von Verknüpfungen zwischen Computern und dynamischen Containern können Sie anhand der IP-Adressen von Computern Pfade zwischen Computern definieren. Wenn die IP-Adresse eines Computers geändert wird, so dass dieser Mitglied eines anderen dynamischen Containers wird, wird auch der Pfad zu diesem Computer geändert.

Hinweis: Die Mitgliedschaft in dynamischen Containern von DTS WorldView unterstützt nur IPv4-Adressbereiche.

Fehlermeldungen

Bei jeder verwalteten DTS-Übertragung, die fehlschlägt, wird die Fehlermeldung an den TOS übergeben. Anwendungen, die DTS verwenden, können diese Fehlermeldung vom TOS abrufen und für die Benutzer anzeigen. Externe Filter stellen ausführliche Fehlerinformationen zur Verfügung, die bei der Identifizierung und Korrektur von Problemen behilflich sind.

Unterstützung für das Übertragen großer Dateien

DTS sieht keine Dateigrößenbeschränkungen vor, aber das Dateisystem des Betriebssystems könnte solche Beschränkungen vorsehen. In den meisten älteren Betriebssystemen ist die Größe der Dateien, die im Dateisystem gespeichert werden können, auf 2 GB beschränkt. Neuere Betriebssysteme haben diese Beschränkung überwunden, so dass DTS auf solchen Systemen Dateien oder Verzeichnisse, die größer als 4 GB sind, übertragen kann.

Hinweis: Weitere Informationen über Dateisystemspezifikationen für die Unterstützung großer Dateien finden Sie in den Unterlagen Ihres Betriebssystems.

PIF-Installationspakete für UNIX

DTS-Installationsprogramme für UNIX verwenden das PIF-Format (Product Interchange Format), das CA-Standardformat zum Packen und Installieren von Softwarelösungen auf UNIX-Systemen. Entwickler erstellen PIF-Installationspakete unter Verwendung des CA-Hilfsprogramms Software Manager Installer für UNIX, das im Folgenden kurz als PIF-Installer bezeichnet wird. Der PIF-Installer steht ebenfalls als Bestandteil des PIF-Installationspakets der CA-Lösung zur Verfügung. Bei der Ausführung des PIF-Installationspakets ermöglicht der PIF-Installer einfaches und effizientes Installieren und Entfernen der Lösung auf den UNIX-Zielcomputern.

Hinweis: Weitere Informationen finden Sie im *Administratorhandbuch für PIF Packager und Installer* .

Integration von DTS und CA Common Services

Für DTS werden CA Common Services (CCS) nicht vorausgesetzt, jedoch ist DTS ohne diese Lösung auf die Funktionen beschränkt, die keine CCS erfordern oder verwenden. DTS bietet zusätzliche Funktionen durch die Integration in die WorldView-Komponente von CCS, die optional bei der Installation einer CA-Client-Lösung, die DTS beinhaltet, installiert werden kann.

Vorhandene Installationen von CCS-Komponenten erfüllen diese Anforderungen. Die besten Ergebnisse erzielen Sie, wenn Sie die aktuelle Version der CCS-Komponente, die Sie verwenden oder planen zu verwenden, aus den CA Common Services-Dateien installieren, die im Lieferumfang des Installationsprogramms Ihrer CA-Client-Lösung enthalten sind.

Hinweis: Sie können die Funktionen von CCS nicht verwenden, wenn Sie CA Common Services nicht auf mindestens einem Computer in Ihrem DTS-Netzwerk installieren.

Wichtig! Wenn CCS aktualisiert wird, indem entweder Unicenter DSM oder CA IT Client Manager r11.6 installiert wird, und wenn die Discovery zuvor unter CCS r3.0 mit kurzen Namen durchgeführt wurde (z. B. mithilfe des Befehls "dscvone -n"), muss die nachfolgende Discovery mit aktivierter Option "remove suffix" ausgeführt werden. Anderenfalls gehen zuvor erkannte Objekte und mit ihnen hergestellte DTS-Verknüpfungen in der 2D-Karte verloren. Dies liegt daran, dass die CSS-Komponente beim Upgrade auf r11.6 automatisch das Netzwerk neu erkennt und neue TCP/IP-Objekte mit vollständig qualifizierten Domännennamen anstelle der ursprünglichen Namen erstellt.

Um dies zu verhindern, muss die Option 'remove suffix' für "dscvrbe" (klassische Discovery) nach der Installation von Unicenter DSM oder CA ITCM mit Hilfe der Option "-3" wie folgt aktiviert werden:

```
dscvrbe -3 <zu entfernende Erweiterung>
```

Beispiel:

```
dscvrbe -3 ca.com
```

Beachten Sie, dass für Continuous Discovery in CCS 11.2 die Option 'remove suffix' nicht vorhanden ist.

Hinweis: Weitere Informationen zu allen Upgrades finden Sie im Kapitel "Aktualisierungs- und Migrationsüberlegungen" im *Implementierungshandbuch*.

WorldView

Wenn Sie CA Common Services in Ihrem Netzwerk installieren, wird DTS nahtlos integriert. CA Common Services bietet WorldView, Enterprise Discovery, Business Process Views™, 2D-Karten, ObjectView, MDB und andere Komponenten, die für DTS wichtige Funktionen wie Routing, Container, dynamische Container, Links, Drosselung und zahlreiche Protokolle zur Datenübertragung bereitstellen.

Sie können DTS mit WorldView und den folgenden Funktionen, die mit DTS installiert werden, verwalten:

- Zahlreiche Business Process Views in WorldView
- Kontextmenüs, damit diese DTS-spezifische Optionen enthalten
- Verschiedene DTS-serverspezifische Formulare (in der Regel über Kontextmenüs)

WorldView bietet folgende Funktionen, die in DTS zur Anzeige und Verwaltung Ihrer Netzwerkressourcen verwendet werden können:

Business Process Views

Während des Auto Discovery-Prozesses von DTS wird im Ordner der verwalteten Objekte von WorldView, der die erkannten DTS-Manager und -Agenten enthält, automatisch ein DTS Business Process View erstellt. DTS-Administratoren können mit Hilfe dieses Business Process View eine DTS-Netzwerktopologie erstellen. In dieser Topologie können Sie angepasste Übertragungsrouten konfigurieren. Mit dem DTS Business Process View können Sie die Verwaltung von großen Computernetzwerken vereinfachen, die an DTS-Aktivitäten beteiligt sind.

Real World Interface

Mit Hilfe des Real World Interface können Sie in Verwaltungsanwendungen 2D-Grafikdarstellungen der darin verwalteten Ressourcen und der Beziehungen zwischen diesen Ressourcen anzeigen.

2D-Karten

Die zweidimensionale Animation des Real World Interface bietet Administratoren eine realistische Ansicht ihres Unternehmens. Mit Hilfe dieser Ansicht können Administratoren einfacher Probleme lösen, indem sie sich durch das Unternehmen bewegen und den Status ihrer Ressourcen überwachen. Darüber hinaus enthalten die 2D-Karten integrierte geografische Karten, über die Sie verwaltete Ressourcen nach Standort anzeigen können.

DTS-Administratoren können mit Hilfe der 2D-Karten ihre DTS-Ressourcen anzeigen und überwachen sowie eine Netzwerktopologie erstellen.

Enterprise Discovery

Der Enterprise Discovery-Prozess von WorldView findet oder erkennt Netzwerkentitäten und Ressourcen und füllt die MDB mit Objekten, die diese Entitäten und ihre Beziehungen darstellen. Das Real World Interface zeigt diese Objekte und die Entitäten an, die sie darstellen, überwachen und steuern.

DTS-Schnittstellen zu WorldView

Sie können auf die Dialogfelder der DTS-Admin-Clients über Kontextmenüs für Objekte in WorldView zu greifen. DTS Auto Discovery können Sie über die Kontextmenüs der DTS Business Process Views aufrufen.

Installieren und Aktualisieren der Business Process Views

Wenn Sie Data Transport Service auf einem Computer mit CA ITCM installieren, wird normalerweise automatisch das Programm "dtsbpv" ausgeführt. Das Programm "dtsbpv" bestimmt automatisch, ob DTS Business Process Views installiert oder aktualisiert werden müssen oder ob beides erforderlich ist. Das Programm führt anschließend die erforderliche Installation und/oder Aktualisierung der Business Process Views auf diesem Computer durch.

Das Programm "dtsbpv" fügt also in der MDB gespeicherte Data Transport Service-Klassen und -Objekte hinzu oder aktualisiert diese. Normalerweise wird die Installation oder Aktualisierung dieser Business Process Views automatisch, also ohne Benutzereingabe, während der Data Transport Service-Installation durchgeführt.

Post-Installationstasks

Manchmal wird das Programm "dtsbpv" während der Data Transport Service-Installation jedoch nicht erfolgreich ausgeführt.

Wenn Sie nicht sicher sind, ob das Programm "dtsbpv" erfolgreich beendet wurde oder wissen, dass es fehlschlug, sollten Sie es manuell ausführen. Auch wenn die Erstinstallation der Business Process Views erfolgreich war, können Sie sie später gegebenenfalls erneut installieren. Eine erneute Installation der Business Process Views kann beispielsweise erforderlich sein, wenn die Data Transport Service NOS-Klassen neu initialisiert werden.

Hinweis: Bei der Ausführung des Programms "dtsbpv" werden alle zuvor eingerichteten Data Transport Service-Klassen und -Objekte gelöscht und durch ein leeres Data Transport Service-Framework ersetzt.

Hinweis: Führen Sie das Programm "dtsbpv" nur auf Computern aus, auf denen CA ITCM und der Data Transport Service Network Object Server (NOS) installiert wurden.

Ausführen von "dtsbpv" über die Befehlszeile

Geben Sie den folgenden Befehl ein, um das Programm "dtsbpv" über die Befehlszeile auszuführen:

```
dtsbpv
```

Installieren und Neuinstallieren der Business Process Views

Wenn Sie Ihre Data Transport Service Business Process Views auf einem Computer deinstallieren (dtsbpv -u) und erneut installieren möchten, führen Sie den folgenden Befehl über die Befehlszeile aus:

```
dtsbpv -u  
dtsbpv
```

Weitere Informationen:

[Business Process Views-Installation schlägt fehl](#) (siehe Seite 92)

Enterprise-Management

DTS nutzt viele Enterprise-Management-Funktionen, darunter Event Management und CCS-Kalender.

Event Management

Event Management sorgt für eine automatisierte Verarbeitung von Nachrichten und Ereignissen. Die Event Management-Konsole enthält ein Fenster zur Enterprise Management-GUI, die das Auftreten von Systemereignissen überwacht. DTS-Ereignisse wie das Starten und Beenden der DTS-Server, die Anfrage einer Übertragung an ein Computerobjekt, das nicht gefunden werden kann, DTS-Fehler und Sicherheitsüberprüfungsfehler werden ebenfalls überwacht. Meldungen, die von DTS-Ereignissen generiert wurden, werden automatisch an die Event Management-Konsole gesendet, wo sie anhand eines bestimmten Präfixes identifiziert werden.

Je nach den Anforderungen Ihres Standorts können Sie Event Management so konfigurieren, dass Ereignismeldungen auf einzelnen Servern verarbeitet oder an einen zentralen Server oder andere Event Management-Server umgeleitet werden. Sie können verknüpfte Meldungen netzwerkweit erfassen und auf einer einzelnen Konsole anzeigen oder nach Bedarf an mehrere Standorte senden.

Über Event Management können Sie bestimmte für Sie wichtige Meldungen identifizieren und anschließend die Aktion festlegen, die durchgeführt werden soll, wenn die Meldungen auftreten. Sie können die Meldungen so verbessern, dass ihre Quelle besser verfolgt wird, oder sie an die Bedürfnisse Ihres Standorts anpassen.

Hinweis: In CA ITCM verwendet DTS die Event Management-Komponente nur indirekt. DTS ist in Common Application Framework (CAF) integriert, an das Ereignisse weitergeleitet werden, und CAF leitet die Ereignisse an Event Management weiter.

CCS-Kalender

Die DTS-Implementierung von Event Management enthält CCS-Kalender, die die Enterprise Management-Komponente bereitstellt. Mit CCS-Kalendern kann der SOS sich wiederholende Übertragungen planen. Ohne Kalender könnte DTS nur einmalige Übertragungen planen.

Mit Kalendern können Zeitpläne mit Datums- und Uhrzeitinformationen erstellt werden, anhand derer Sie verschiedene Jobs oder Funktionen starten können. DTS verwendet Kalender, um komplexe Zeitpläne für Datenübertragungen zu erstellen. Mit Hilfe dieser Zeitpläne können Sie Übertragungen zu einem zukünftigen Datum oder Zeitpunkt planen, regelmäßig geplante Übertragungen erstellen und die Ausführung von Übertragungen zu einer bestimmten Uhrzeit verhindern.

Hinweis: Auf die Zeitplanungsfunktionen kann über die Client-API zugegriffen werden.

Datenübertragungen

Mit Hilfe der Funktionen von DTS können Sie Datenübertragungen über verschiedene Plattformen und Übertragungsprotokolle erstellen und auslösen. Sie können diese Übertragungen unmittelbar aktivieren oder für einen späteren Zeitpunkt planen.

Darüber hinaus ist es möglich, aktive Datenübertragungen zu überwachen und deren Status anzuzeigen. Überwacht werden u. a. der prozentuale Anteil der erfolgten Übertragung sowie die Gesamtanzahl der übertragenen Pakete. Aktive Datenübertragungen können ausgesetzt, abgebrochen oder wiederaufgenommen werden, wenn sie vorher ausgesetzt waren.

Bei DTS stehen Ihnen die hier erläuterten Datenübertragungsfunktionen über die Client-API zur Verfügung. DTS dient als zu Grunde liegender Dienst für CA-Lösungen wie CA ITCM. Diese Anwendungen bieten über eigene grafische Benutzeroberflächen zusätzlichen Zugriff auf die Datenübertragungsfunktionen.

Weitere Informationen über CA-Anwendungen, die eine grafische Benutzeroberfläche für DTS bereitstellen, erhalten Sie von Ihrem CA-Vertriebsbeauftragten.

Alternatives Routing

Wenn eine Übertragung über die effizienteste Route erfolgreich ist, wird keine alternative Route ausprobiert. Wenn die effizienteste Route jedoch fehlschlägt, werden die alternativen Routen mit einer bestimmten Anzahl von Wiederholungen oder so lange ausprobiert, bis die Übertragung abgeschlossen ist oder fehlschlägt.

Die Effizienz jeder möglichen Route wird von DTS-Netzwerk-Administratoren basierend auf deren Beobachtung der Netzwerkleistung zugewiesen.

Diskrete Übertragungen

Diskrete Übertragungen werden im Hintergrund gesendet oder empfangen, wenn die sendenden und empfangenden Computer nicht stark ausgelastet sind. Je nach Auslastung der Computer bestimmt der DTS Agent, wann die Übertragung gesendet wird, und berechnet die optimale Übertragungsrates, so dass die diskrete Übertragung die Computerleistung und die Benutzerproduktivität nur minimal beeinflusst.

Die für eine diskrete Übertragung verwendete Rate wird automatisch und dynamisch vom DTS-Agenten bestimmt. Der DTS-Agent überwacht die Auslastung (sowohl CPU-Nutzung als auch die Netzwerkauslastung des Computers) der sendenden und empfangenden Computer. Wenn ein Computer nur gering ausgelastet ist, verwendet der DTS Agent die freien Ressourcen. Wenn die Auslastung jedoch zunimmt, tritt der Agent Ressourcen ab, so dass andere Tasks auf dem Computer vorrangig ausgeführt werden. Auf diese Weise optimiert der diskrete Modus die Computerleistung bei der Durchführung von Übertragungen.

Maximale Anzahl von Übertragungen pro Job in einer Fanout-, Broadcast- oder Multicast-Übertragung

Bei der Aktivierung einer Fanout-, Broadcast- oder Multicast-Übertragung können Sie für jeden erzeugten Übertragungsjob die maximale Anzahl der zulässigen Übertragungen angeben. Wenn die Anzahl der im Fanout-, Broadcast- oder Multicast-Modus erzeugten Übertragungen den maximal zulässigen Wert überschreitet, erstellt DTS automatisch die zusätzliche Anzahl Übertragungsjobs, die erforderlich sind, um alle generierten Übertragungen aufzunehmen.

Hinweis: Detaillierte Informationen finden Sie im *Referenzhandbuch für DTSCLI-Befehle*.

Konfiguration des Staging-Verzeichnisses

DTS bereinigt bzw. löscht die Staging-Dateien von erfolgreichen Übertragungen automatisch. Bei fehlgeschlagenen oder abgebrochenen Übertragungen ermittelt DTS mit dem Parameter "StagingFileLifetime", ob und wann die Staging-Dateien von solchen Übertragungen gelöscht werden sollen.

Hinweis: Ausführliche Informationen hierzu finden Sie in der *Hilfe zum Data Transport Service WorldView-Admin-Client*.

Auditing

Die Audit-Meldungen für häufig eintretende Ereignisse, wie das Fehlschlagen des DTS Agenten bzw. des TOS oder den Abbruch eines Übertragungsjobs, können von DTS-Administratoren angepasst werden. Dabei wird die Standardmeldung, die von DTS normalerweise bei Vorliegen derselben Bedingungen an die Common Event-Komponente von CA ITCM ausgegeben würde, durch die angepasste Meldung ersetzt.

Wenn beispielsweise vor einer solchen Anpassung der TOS während des Normalbetriebs fehlschlägt, sendet DTS die Standardmeldung "Transfer Object Server-Fehler" an die TOS-Protokolldatei und an CA ITCM. Wenn Sie jedoch das *Audit-Token* TOS_FAIL= anpassen, sendet DTS die benutzerdefinierte Meldung (anstelle der Standardmeldung) an CA ITCM.

So können Administratoren mit Hilfe benutzerspezifischer Meldungen Fehler flexibler überwachen und handhaben. Wenn z. B. eine Übertragung fehlschlägt oder ausgesetzt wird, kann der TOS für die Ausgabe von Quelle, Ziel und Text der angepassten Meldung konfiguriert werden.

Hinweis: In CA ITCM werden Kommunikation, Auditing, Tracing, Ereignismanagement, Komprimierung, Verschlüsselung usw. von allgemeinen Komponenten im Common Application Framework (CAF) verarbeitet. Einen Überblick hierzu finden Sie im *Implementierungshandbuch*.

Weitere Informationen:

[Anpassen von Audit-Meldungen](#) (siehe Seite 62)

[Ändern der Audit-Ebenen](#) (siehe Seite 59)

Handhabung von DHCP- und Modemverbindungen

Für die DTS-Agenten stehen Benachrichtigungsparameter zur Verfügung, die über DFÜ-Computer oder DHCP (Dynamic Host Configuration Protocol) eine Verbindung zum TOS herstellen. Mit den Benachrichtigungsparametern können Agenten, die selten oder nur kurz mit dem Netzwerk verbunden sind, nach ausstehenden Übertragungen suchen, sobald sie eine Verbindung mit einem TOS herstellen.

HTTP-Protokollunterstützung

Das HTTP-Protokoll ist das gebräuchlichste Protokoll zum Übertragen von Daten von World Wide Web-Servern an Browser. Selbst wenn auf dem Server kein DTS-Agent installiert ist, kann ein DTS-Benutzer Übertragungen erstellen, verwalten und durchführen, um Daten von einem HTTP-Server oder dem zugehörigen Proxy-Server zu empfangen. DTS unterstützt auf diese Weise das Herunterladen von Dateien aus dem Internet.

Hinweis: Weitere Informationen finden Sie in der *Hilfe zum Data Transport Service WorldView-Admin-Client*.

Protokollauswahl

Sie können die DTS-Agenten so konfigurieren, dass bei ihrem Start nur die von Ihnen angegebenen Protokolle anstatt alle von DTS unterstützten Protokolle geladen werden. Dadurch laden Slave-Agenten nur die Protokolle, die für die Ausführung der Übertragung erforderlich sind.

Externe Protokolle

Neben den von DTS bereitgestellten Protokollen können Sie auch externe Protokolle verwenden, d. h. Protokolle, die auf dem ausgewählten Computer installiert sind, jedoch nicht von DTS bereitgestellt werden. Außerdem können Sie Protokollbibliotheken für Protokolle schreiben, die gegenwärtig nicht unterstützt werden.

Kapitel 2: Architektur

Neben einer Übersicht über die Architektur von Data Transport Service enthält dieses Kapitel kurze Beschreibungen der verschiedenen Komponenten und einiger Funktionen.

Dieses Kapitel enthält folgende Themen:

[Überblick](#) (siehe Seite 25)

[DTS-Manager](#) (siehe Seite 26)

[DTS-Agent](#) (siehe Seite 31)

[DTS-Client-API](#) (siehe Seite 37)

[DTS-Browser](#) (siehe Seite 38)

[DTS-Sicherheit](#) (siehe Seite 38)

Überblick

DTS ist hinsichtlich der Konfigurationsmöglichkeiten der unterschiedlichen Komponenten im Netzwerk ein äußerst flexibler Dienst. Vor der Konfiguration Ihres DTS-Netzwerks müssen Sie die Funktion der einzelnen Komponenten kennen. Die zentrale Komponente von DTS, der Data Transport-Manager, fungiert als verteilter Server. Anwendungen stellen zum Data Transport-Manager eine Verbindung her und verwenden ihn zur Ausführung und Planung von Datenübertragungen. Der DTS Agent muss auf allen Computern installiert sein, die an der Übertragung von tatsächlichen Daten beteiligt sind.

In CA ITCM werden Kommunikation, Auditing, Tracing, Ereignismanagement, Komprimierung, Verschlüsselung usw. von allgemeinen Komponenten innerhalb vom Common Application Framework (CAF) behandelt. Einen Überblick hierzu finden Sie im *Implementierungshandbuch*.

Hinweis: Frühere Versionen von DTS, die auf Unicenter DSM r11.1 aktualisiert wurden, lassen sich nicht in die CA Common Services integrieren. Das bedeutet, dass alle erweiterten DTS-Netzwerkkonfigurationen, die mit einer früheren Version der CCS eingerichtet wurden, in r11.1 nicht zur Verfügung stehen. Wird allerdings eine vorherige Version auf Unicenter bzw. CA ITCM r11.6 aktualisiert, gilt dies nicht, d. h., die vorhandene Netzwerkkonfiguration ist dann verfügbar.

Hinweis: Wird CA ITCM r12 erfolgreich über CCS r3.0 installiert, sind in CCS konfigurierte DTS-Daten jedoch nicht mehr verfügbar.

DTS-Manager

Die DTS-Netzwerkumgebung besteht aus mehreren Domänen, die jeweils über einen DTS-Manager verfügen. Der DTS-Manager besteht aus den folgenden Manager-Komponenten, von denen jede eine spezifische Aufgabe hat:

- Network Object Server (NOS)
- Transfer Object Server (TOS)
- Schedule Object Server (SOS)

Hinweis: Mit den Bezeichnungen "Objektserver", "DTS-Server" und "Server" wird in der gesamten Dokumentation auf Transfer Object Server (TOS), Network Object Server (NOS) und Schedule Object Server verwiesen. Entsprechend der DSM-Terminologie handelt es sich jedoch formal um DTS-Manager.

Network Object Server

Der Network Object Server (NOS) verwaltet den DTS-Computer sowie die Computergruppendaten, die in WorldView(tm), einem Bestandteil von MDB gespeichert sind. Mit den in den Objekten gespeicherten Eigenschaften von Informationen können Sie komplexe Routing-Topologien im Netzwerk festlegen. Darüber hinaus verwendet der TOS den NOS, um Routing-Topologien und optimale Übertragungspfade im DTS-Netzwerk herzustellen.

Normalerweise bearbeiten Sie die in der MDB gespeicherten Objekte nicht über die Client-API. Normalerweise wird WorldView verwendet, um DTS-Netzwerkobjekte zu konfigurieren und zu verwalten.

Der von DTS verwendete Optimierungsprozess aus vier Phasen sorgt für die effizienteste Datenübertragung. Der NOS ist für die Durchführung der Phasen 1 und 2 des Optimierungsprozesses verantwortlich, nämlich die Netzwerkroutenanalyse und Übertragungseigenschaftenauflösung.

Weitere Informationen:

[Phase 1: Netzwerkroutenanalyse](#) (siehe Seite 69)

[Phase 2: Übertragungseigenschaftenauflösung](#) (siehe Seite 70)

NOS-Klassen

NOS verwaltet folgende Klassen:

Computerklasse (DTMachine)

Ein Computerobjekt steht für einen beliebigen Computer, der Teil einer DTS-Domäne ist, oder einen Computer, auf dem ein DTS-Server, -Agent oder beides installiert ist. Computerobjekte definieren Eigenschaften, die mit dem eigentlichen Computer verknüpft sind, wie Name und Beschreibung, sowie Eigenschaften, die Übertragungseigenschaften definieren, die Datenübertragung verwenden. Wenn ein Computer mehrere Kommunikationsschnittstellen besitzt, verweist das Computerobjekt möglicherweise auf eines oder mehrere Schnittstellenobjekte. DTMachine ist eine virtuelle, erweiterte übergeordnete Klasse mit den realen untergeordneten Klassen Host, Workstation und nicht qualifiziertem TCP. Wenn Sie DTMachine verwenden, müssen Sie also nicht wissen, ob ein bestimmter Computer als Host, Workstation oder nicht qualifiziertes TCP-Objekt klassifiziert ist.

Die MDB bietet oder enthält keine DTMachine-Klasse. Der NOS stellt DTMachine bereit. DTMachine vereinfacht die Verwendung von Objekten in der MDB, die Computern entsprechen, und erweitert diese Objekte um viele DTS-Dienstspezifische Eigenschaften. Die Eigenschaften von Computerobjekten wirken sich auf die Art und Weise der Datenübertragung aus, und Sie können diese Eigenschaften an Ihre jeweiligen Bedürfnisse anpassen. Sie können beispielsweise die entsprechende Eigenschaft ändern, um die von einem Computer ausgehende Datenübertragungsrate zu begrenzen, die auf dem Computer verfügbaren Protokolle anzugeben oder festzulegen, dass ein Computer für den Empfang einer Broadcast-Datenübertragung zur Verfügung steht.

Computergruppenklasse (DTMachineGroup)

Ein Computergruppenobjekt besteht aus einer logischen Gruppierung von Computern, anderen Computergruppenobjekten oder beidem. Sie können diese Objekte einrichten. Mit Computergruppenobjekten können Benutzer und Administratoren ihre eigene eindeutige, logische Ansicht einer DTS-Domäne erstellen. Computergruppenobjekte sind unabhängig von der definierten Netzwerktopologie und haben keine Auswirkungen auf Übertragungsrouten innerhalb des Netzwerks.

Computercontainerklasse (DTContainer)

Ein Computercontainerobjekt definiert allgemeine Übertragungseigenschaften für mehrere Computerobjekte. Zu diesen Einstellungen gehören die Protokoll- und andere Kommunikationseinstellungen, die die Computer während einer Datenübertragung verwenden. Administratoren können mit Hilfe von Computercontainerobjekten Eigenschaften für eine Gruppe von Computerobjekten festlegen, indem sie die Computerobjekte in ein Containerobjekt ablegen und anschließend die Eigenschaften des Computercontainerobjekts angeben.

Dynamische Containerklasse (DTDynamicContainer)

Die dynamische Containerklasse (DTDynamicContainer) funktioniert ähnlich wie die DTContainer-Klasse, weist jedoch eine zusätzliche Eigenschaft auf: eine Reihe von Adressen oder ein Subnetz, das die Mitglieder des Containers definiert. Alle Agenten, deren IP-Adresse in diesem Bereich liegt, werden Mitglieder des dynamischen Containers.

Mit Hilfe von dynamischen Containern können Benutzer Routen zwischen Computern und einem dynamischen Container erstellen. In einem dynamischen Container werden Objekte abgelegt, deren Adressen sich mit der Zeit ändern, z. B. Computer, die DHCP oder DFÜ-Verbindungen verwenden. Wenn Sie DTS-Objekte in WorldView anzeigen und es sich bei dem von Ihnen ausgewählten DTS-Objekt um einen dynamischen Container handelt, werden im Feld "Klasse" der DTDynamicContainer und neben der Registerkarte "Objektdetails" eine zweite Registerkarte ("Zugehörigkeit") angezeigt. Auf dieser Registerkarte können Sie die einzelnen Adressen und Adressbereiche anzeigen und ändern, die diesem dynamischen Container angehören.

Hinweis: Die Mitgliedschaft in dynamischen Containern von DTS WorldView unterstützt nur IPv4-Adressbereiche.

Verknüpfungsklasse (DTLink)

Ein Verknüpfungsobjekt definiert eine DTS-Kommunikationsverknüpfung zwischen zwei verschiedenen Computern oder Computercontainerobjekten. DTS-Administratoren definieren diese Verknüpfungen, die Quell- und Zielcomputer identifizieren, mit gemeinsamen Übertragungseigenschaften, die dem Link zugeordnet sind. Verknüpfungen definieren feste Datenübertragungsrouten innerhalb des Unternehmens.

Schnittstellenklasse (DTInterface)

Ein Schnittstellenobjekt definiert eine physische Schnittstelle, die mit einem bestimmten Computer verknüpft ist. Sie können der Schnittstelle spezifische Protokollmerkmale zuordnen. Durch die Zuweisung einer Prioritätseigenschaft zur Schnittstelle können die Benutzer die Reihenfolge der Auswertung der Schnittstellen festlegen, wenn sie die Route und Eigenschaften einer Übertragung angeben. Schnittstellen, die mit dem antwortenden Computer verknüpft sind, werden nacheinander in der angegebenen Reihenfolge mit denen des als Initiator agierenden Computers verglichen, bis eine Schnittstelle mit übereinstimmenden Merkmalen gefunden wird.

Transfer Object Server (TOS)

Der Transfer Object Server (TOS) ist für das Auslösen, Steuern und Überwachen sämtlicher von Benutzern angeforderter Datenübertragungen sowie für das Entgegennehmen und Verarbeiten von Anforderungen der Client-API verantwortlich. Wenn der TOS eine Datenübertragung aktiviert, sendet er eine Meldung an den auslösenden DTS Agent und weist diesen an, die Daten zu übertragen. Der TOS ist anschließend für die Verarbeitung der Fortschritts- und Statusmeldungen verantwortlich, die vom auslösenden Agent zurückgegeben werden.

Der TOS optimiert diese Anforderungen, indem die Netzwerkressourcen so effizient wie möglich eingesetzt werden. Auf diese Weise werden Hops (Zwischenknoten), Fanouts und Broadcasts verwaltet. Der TOS verwendet jegliche verfügbare Informationen zur Netzwerktopologie, die er vom NOS erhält, und weist den DTS-Agenten auf dem sendenden Computer an, die Datenübertragung durchzuführen. Zusätzlich können Anwendungen mit Hilfe des TOS die von ihnen gesendeten Übertragungen überwachen und steuern.

Sie können eine Verbindung mit dem TOS über die Client-API aufbauen und erstellen Filter-, Übertragungs- und Übertragungsgruppenobjekte. Sie richten die Objekteigenschaften entsprechend ein, um Ihre Datenübertragungsanforderungen vollständig zu definieren. Anschließend können Sie dann die Übertragungsgruppenobjekt-Methode "ACTIVATE" aufrufen, um die von Ihnen definierten Übertragungen durchzuführen. Der TOS speichert alle diese Objekte dauerhaft in seiner eigenen lokalen Objektdatenbank, die als Transfer Object Repository (TOR) bezeichnet wird.

Hinweis: Mit Hilfe der DTS-Befehlszeilenschnittstelle können Agent-zu-Agent-Übertragungen ohne TOS durchgeführt werden.

Der TOS greift direkt über sein TOR auf die MDB zu und ruft über NOS Informationen von WorldView (ebenfalls Teil der MDB) ab. Anhand der von NOS zurückgegebenen Netzwerkobjekteigenschaften wird entschieden, auf welche Weise Ihre Daten am besten übertragen werden.

Der von DTS verwendete Optimierungsprozess aus vier Phasen sorgt für die effizienteste Datenübertragung. Der TOS ist für die Durchführung der Phasen 3 und 4 des Optimierungsprozesses verantwortlich, nämlich das Auflösen doppelter Übertragungen bzw. die Auswahl des Übertragungsverfahrens.

Weitere Informationen:

[Phase 3: Auflösen doppelter Übertragungen](#) (siehe Seite 73)

[Befehlszeilenschnittstelle](#) (siehe Seite 12)

[Phase 4: Auswahl des Übertragungsverfahrens](#) (siehe Seite 73)

TOS-Klassen

TOS verwaltet die folgenden Klassen:

Übertragungsklasse (DTTransfer)

Das Übertragungsobjekt definiert die Durchführung der Datenübertragung. Es umfasst sämtliche Informationen, die erforderlich sind, um die Übertragung der angegebenen Daten von einem Ort zu einem anderen durchzuführen. Es stellt ferner Eigenschaften und Methoden bereit, mit denen der Benutzer die Datenübertragung überwachen und steuern kann. Übertragungsobjekte enthalten Referenzen auf Filterobjekte und Computer. Wenn ein Übertragungsobjekt erstellt wird, verwendet der TOS die Eigenschaften des Standardübertragungsobjekts für die neue Übertragung. So können Sie die Mindestanzahl von Eigenschaften festlegen, die eine Ausführung der Übertragung ermöglichen. Bei diesen Eigenschaften handelt es sich um Eingabe (Quelldaten), Ausgabe (Zieldaten), Initiator (Quellcomputer) und Responder (Zielcomputer).

Übertragungsgruppenklasse (DTTransferGroup)

Ein Übertragungsgruppenobjekt besteht aus einer benutzerdefinierten Gruppe von Übertragungsobjekten. Sie können diese Übertragungen nacheinander oder als Gruppe aktivieren (so werden die Aktivierungsalgorithmen des TOS in vollem Umfang genutzt). Die Übertragungsobjekte können nicht einzeln aktiviert, abgebrochen, ausgesetzt, wiederaufgenommen oder zurückgesetzt werden. Diese Methoden sind nur auf Übertragungsgruppenobjekte anwendbar.

Filterklasse (DTFilter)

Filterobjekte definieren einige Vorgänge, die mit den zu übertragenden Daten ausgeführt werden. Wenn die Übertragung aktiviert ist, funktioniert dieser Vorgang entweder für die Datei (dateibasiert) oder für Datenpuffer (paketbasiert). Filterobjekte sind mit Übertragungsobjekten verbunden und stellen die eigentlichen Filter bzw. die Filterung dar, die auf die Daten angewendet wird, bevor, während oder nachdem diese Daten gelesen und/oder geschrieben werden. Diese Filter können das Einlesen von Text sowie die Verschlüsselung und Komprimierung von Daten betreffen. Die Eigenschaften der Filterobjekte legen den zu verwendenden Filterungstyp fest.

Schedule Object Server (SOS)

Der Schedule Object Server (SOS) wird dazu verwendet, Zeitplanungsanfragen zu erstellen und zu steuern, die den Zeitpunkt von Übertragungen festlegen. Diese Zeitplanungsdaten werden in Form von Zeitplan-Objekten in der lokalen Datenbank des Schedule Object Servers abgelegt. Der Schedule Object Server überwacht diese Objekte und weist den Transfer Object Server an, die vom Zeitplan referenzierte(n) Übertragungsgruppe(n) bei Fälligkeit der Datum-/Uhrzeitinformationen zu aktivieren. Auf die Zeitplanungsfunktionen kann über die Client-API zugegriffen werden.

Hinweis: In CA ITCM ist der SOS standardmäßig deaktiviert. Um ihn zu aktivieren, geben Sie den Befehl "caf enable dtssos" über ein Befehlszeilenfenster oder die Option "Ausführen" im Windows-Startmenü ein. Nähere Informationen zu dem Befehl erhalten Sie, wenn Sie "<command> /?" in der Befehlszeile eingeben.

UNIX-Manager

Alle Komponenten von DTS-Manager (TOS, NOS und SOS) werden nur unter Windows 2003 ausgeführt. Unter UNIX/Linux werden Manager nicht unterstützt.

DTS-Agent

Der DTS Agent ist für die physische Übertragung der Daten verantwortlich. Er führt diese Übertragung auf Anforderung des TOS durch. Über die CLI werden mehrere Datenübertragungsprotokolle, wie TCP/IP, UDP/IP, PPP, SNA, SPX, Broadcast und Multicast, vom DTS Agenten unterstützt.

Hinweis: DTS unterstützt nicht die neueste Version des PPP-Kommunikationsprotokolls, PPPv6.

Während jeder Datenübertragung übernimmt ein Agent zwei Persönlichkeitseigenschaften, die seine Rolle (und seine Aufgaben) während des Übertragungszyklus definieren. Diese Eigenschaften schreiben vor, dass der Agent entweder als Initiator oder Responder und entweder als Sender oder Empfänger agiert.

Initiator

Wenn der Agent ein Initiator ist, weist der TOS den Agenten direkt an, die Datenübertragung auszuführen. Der Agent ist als Initiator für die Einleitung der Verbindung zu dem anderen Agenten (dem Responder) sowie für die Weiterleitung von Informationen über den Fortschritt und Änderungen im Status der Übertragung an den TOS verantwortlich.

Responder

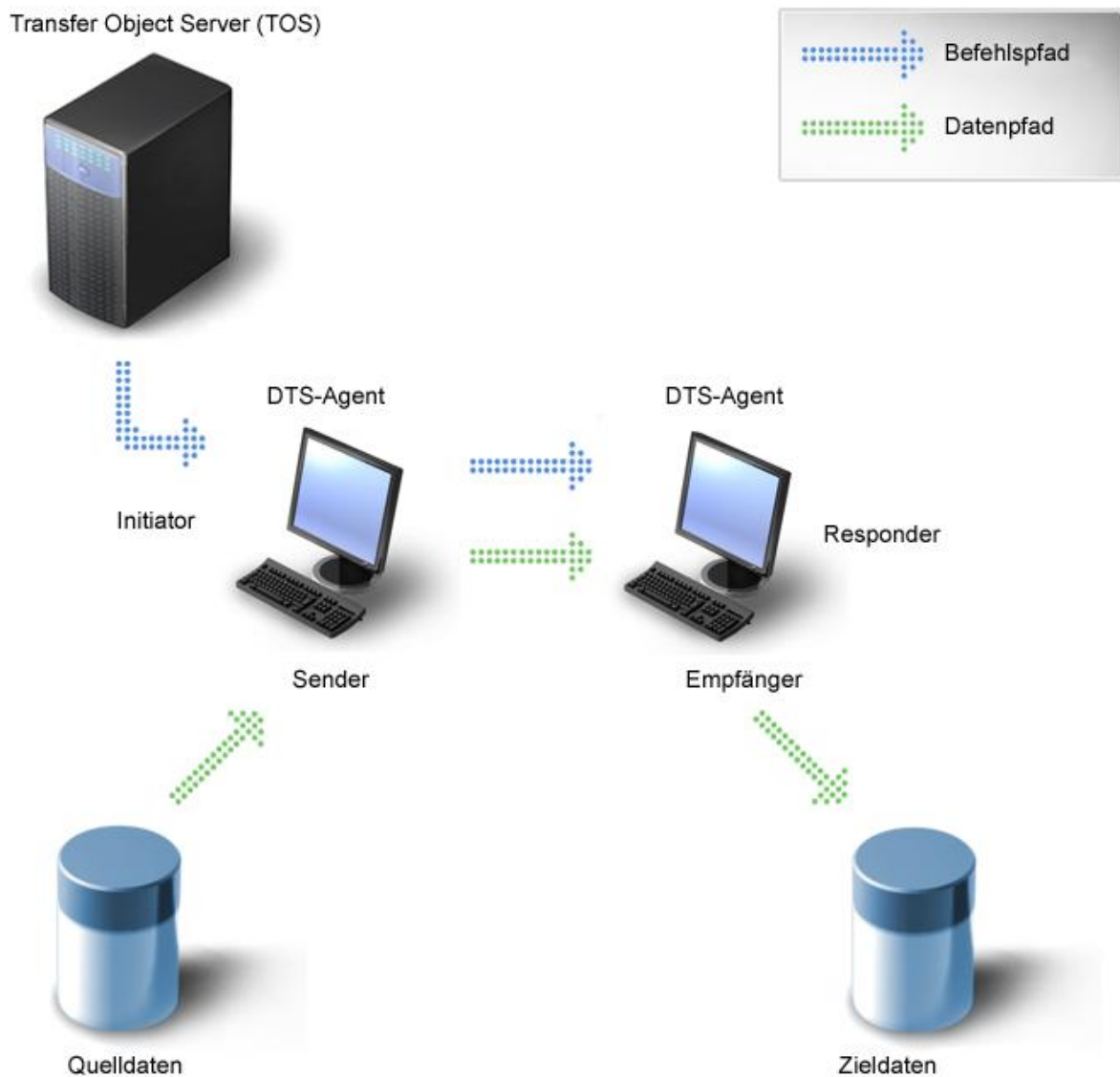
Wenn der Agent ein Responder ist, hat sich ein Initiator-Agent (und nicht der TOS) mit ihm verbunden und ihm mitgeteilt, was er zu tun hat.

Sender- und Empfängeraufgaben

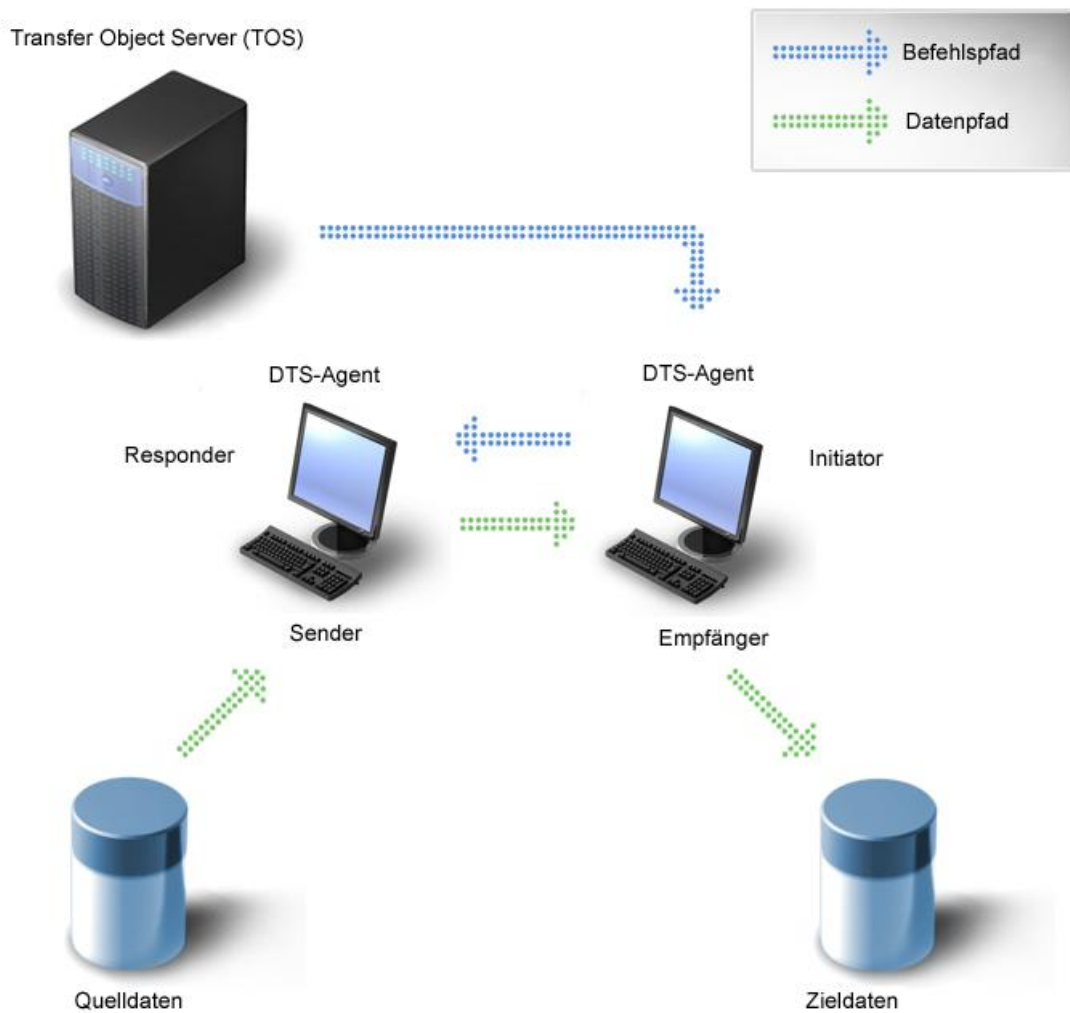
Hinsichtlich der tatsächlichen, physischen Übertragung der Daten ist die Aufgabe des Agenten ziemlich einfach. Als Sender muss der Agent die Quelldaten einlesen und verarbeiten und sie dann an den Empfänger-Agenten weiterleiten. Als Empfänger muss der Agent die Daten vom Sender-Agent in Empfang nehmen, dann verarbeiten und sie anschließend in den Zielspeicherort schreiben.

Hinweis: Ein Initiator-Agent ist normalerweise ein Sender und ein Responder-Agent ist normalerweise ein Empfänger; es kann jedoch auch umgekehrt sein.

Einen typischen Fall, bei dem der Initiator-Agent der Sender und der Responder-Agent der Empfänger ist, zeigt das folgende Schaubild:



Den Fall, bei dem der Initiator-Agent der Empfänger und der Responder-Agent der Sender ist, zeigt die folgende Darstellung:



Filter

Der Filtermechanismus lässt den Agenten Daten lesen, verarbeiten und schreiben. Filter für Dateien und Pakete können Text- bzw. Binärdaten lesen, Daten komprimieren, verschlüsseln, Binärdaten schreiben, Daten dekomprimieren und entschlüsseln usw.

Agenten lesen und senden sich gegenseitig Daten in Form von Blöcken, die als Pakete bezeichnet werden. Ein Paket ist die Menge an Rohdaten, die ein Sender-Agent liest, bevor er Paketfilter anwendet und die Daten durch das Netzwerk zum Empfänger-Agenten schickt. Der Standardwert für die Paketgröße ist ca. 500 KB. Dies bedeutet z. B., dass bei der Abwicklung der Übertragung von Daten im Umfang von 10 MB 20 Datenpakete gelesen und gesendet werden müssen.

Sie können zur Verwendung für Datenübertragungen eigene Filter und entsprechende Filterobjekte erstellen oder verschiedene vordefinierte Datei- und Paketfilter verwenden.

Folgende Typen von DTSCLI-Dateifiltern sind gültig:

- Verzeichnisfilter
- Verschlüsselungsfilter
- Dateiattributfilter

Beim Hinzufügen von Dateifiltern werden unter Umständen auch Paketfilter benötigt. Um ein Verzeichnis zu übertragen, müssen an den Befehl "dtscli" Dateifilter angehängt werden. Wenn Sie versuchen, ein Verzeichnis zu übertragen, ohne einen Verzeichnisfilter hinzugefügt zu haben, erhalten Sie die folgende Fehlermeldung:

```
"Öffnen der Eingabedaten fehlgeschlagen <c:\dtstemp> Fehler=<Berechtigung verweigert>".
```

Folgende Typen von DTSCLI-Paketfiltern sind gültig:

- Binär (Standard) oder Text
- Komprimieren
- Verschlüsseln

Die zwei wichtigsten Paketfilter sind Binär und Text. Verwenden Sie den Textfilter, wenn Sie Textdateien zwischen zwei Computern verschiedener Typen übertragen (zum Beispiel zwischen Windows XP und UNIX). Hiermit ist gewährleistet, dass das Textformat erhalten bleibt. Verwenden Sie in allen anderen Fällen stets Binärfilter.

Hinweis: Binärfilter und Textfilter schließen sich gegenseitig aus: Eine Übertragung kann nur im Text- oder im Binärmodus erfolgen. Eine Kombination ist nicht möglich.

Filter werden in der Regel paarweise verwendet. Der Schreibfilter muss eine Aktion umkehren, die vom Lesefilter ausgeführt wurde. Filter werden in der folgenden Reihenfolge angewandt:

- Datei lesen - Wird beim Lesen der Quelldaten auf eine Datei angewendet.
- Paket lesen - Wird beim Lesen der Quelldaten auf Datenpuffer angewendet.
- Paket schreiben - Wird beim Schreiben der Zieldaten auf Datenpuffer angewendet.
- Datei schreiben: Wird beim Schreiben der Zieldaten auf eine Datei angewendet.

Lesefilter desselben Typs (Datei- oder Paketfilter) werden in der Reihenfolge angewandt, in der sie in der Befehlszeile angegeben werden. Schreibfilter desselben Typs werden in der umgekehrten Reihenfolge ihrer Angabe in der Befehlszeile angewandt.

DTS unterstützt auch Filter für externe Dateien und Pakete.

Beispiel: Übertragen eines Verzeichnisses

- Im folgenden Beispiel wird ein Verzeichnis mit dem Verzeichnisfilter im Kurzformat übertragen:

```
dtsccli -agent ipath=Gold::c:\dtstemp  
"rpath=Silber::c:\dtstemp"  
"f_filters=dir"
```

- In diesem Beispiel wird derselbe Vorgang im Langformat ausgeführt:

```
dtsccli -agent "ipath=Gold::c:\dtstemp"  
"rpath=Silber::c:\dtstemp"  
"f_filters=DIRTREE_READ:DIRTREE_WRITE"  
"p_filters=binary"
```

Beispiel: Übertragen einer Datei als Text

- Im folgenden Beispiel wird die Datei unter Verwendung eines Textfilters im Kurzformat vom Computer "Gold" auf den Computer "Silber" übertragen:

```
dtsccli -agent "ipath=Gold::c:\dtstemp\Datei.quell"  
"rpath=Silber::c:\dtstemp\Datei.ziel"  
"p_filters=text"
```

- In diesem Beispiel wird derselbe Vorgang im Langformat ausgeführt:

```
dtsccli -agent "ipath=Gold::c:\dtstemp\Datei.quell"  
"rpath=Silber::c:\dtstemp\Datei.ziel"  
"p_filters=TEXT_READ:TEXT_WRITE"
```

Hinweis: Textfilter dürfen nur für die Übertragung von Textdateien verwendet werden.

Hinweis: Detaillierte Informationen finden Sie im *Referenzhandbuch für DTSCCLI-Befehle*.

Weitere Informationen:

[Unterstützung für externe Filter](#) (siehe Seite 99)

[Erstellen von Übertragungsobjekten](#) (siehe Seite 53)

DTS-Client-API

Die Client-API von DTS besteht aus einer Bibliothek mit Funktionen, die eine Programmierschnittstelle für die verschiedenen DTS-Funktionen zur Verfügung stellt. Diese Funktionen umfassen Datenübertragung und Zeitplanung, Fehlerprotokollierung und Wiederherstellung sowie Informationen zur Netzwerkkonfiguration und Überwachungsfunktionen.

Die Client-API befindet sich auf der Ebene der Benutzeranwendung und kommuniziert mit den DTS-Servern über eine Kommunikationsverbindung, für die ein Protokoll wie z. B. TCP/IP verwendet wird. Wenn die Client-API Anwendungsanfragen erhält, gibt sie diese Anfragen an die DTS weiter und gibt diese an die aufrufende Anwendung zurück.

Unter Verwendung der Client-API können Anwendungen folgende Aufgaben ausführen:

- Herstellen und Aufheben von Verbindungen zu Objektservern
- Erstellen und Löschen von Objekten (Instanzen erstellen und entfernen)
- Anzeigen und Konfigurieren von Objekten (Eigenschaften abrufen und festlegen)
- Aufrufen von mit den Objekten verknüpften Funktionen (Methoden)
- Abfragen von Objektdatenbanken (Repositories) nach Objekten, die bestimmte Auswahlkriterien erfüllen

Die Client-API bietet ferner eine Reihe von Administrationsfunktionen zum Anzeigen und Aktualisieren sowohl der Manager- als auch der Agent-Laufzeitparameter.

Weitere Informationen:

[Erstellen von Übertragungsobjekten](#) (siehe Seite 53)

DTS-Browser

Wenn Sie eine CA-Lösung mit einer Übertragungs-GUI für DTS installiert haben, können Sie diese Übertragungs-GUI zum Erstellen von Übertragungen verwenden. Hierzu durchsuchen und wählen Sie Laufwerke, Verzeichnisse und Dateien auf Remote-Computern, anstatt die Pfadnamen in der Befehlszeile bzw. in einer Datei manuell einzugeben. Weitere Informationen über die Verwendung der Funktionen des Browsers finden Sie in der Online-Hilfe für die Übertragungs-GUI der von Ihnen als Ergänzung zu DTS verwendeten CA Software.

Hinweis: In allen früheren Versionen von DTS wurde der Browser als Data Object-Agent bezeichnet. Daher verwenden die AS/400-, OS/2- und OpenVMS-Komponenten nach wie vor die Bezeichnung "Data Object-Agent" anstatt "Browser" oder "Browser-Agent".

DTS-Sicherheit

In der DTS-Architektur ist Sicherheit auf verschiedenen Ebenen implementiert.

Data Transport-Manager (DTS-Manager)

Sie können die Sicherheit für jede DTS-Manager-Komponente (TOS, NOS und SOS) und für den DTS Agenten aktivieren.

Bei Aktivierung der Sicherheit (d.h., der Parameter für den Sicherheitsmodus ist auf "fail" gesetzt), müssen Agenten, die eine Verbindung zu einem Server oder Agenten aufbauen, einen gültigen Benutzernamen und ein Kennwort eines bestehenden Benutzers angeben, der bei dem Computer registriert ist, zu dem Sie eine Verbindung herstellen.

Data Transport-Agent (DTS Agent)

Wenn Sie die Sicherheit für einen Agenten aktivieren, müssen sämtliche Datenübertragungen, an denen der Agent beteiligt ist, gültige Benutzername/Kennwort-Kombinationen für den Initiator- und für den Respondercomputer aufweisen.

Daten

Verschlüsselung sorgt für Datensicherheit. Die Daten werden vor der Übertragung verschlüsselt und nach Erreichen des Ziels entschlüsselt. Sie können entweder Paket- oder Dateiverschlüsselungsfilter verwenden.

Weitere Informationen:

[dtscli \(Befehl\)](#) (siehe Seite 13)

Kapitel 3: Implementierung

Die in diesem Kapitel enthaltenen Informationen dienen in erster Linie dazu, einen Einblick in die Anforderungen beim Einrichten eines zentralen DTS-Netzwerks zu geben. Die eigentliche Implementierung wird von CA ITCM ausgeführt, wobei die Komponenten von DTS-Agent und -Manager automatisch an den entsprechenden Stellen installiert werden.

Dieses Kapitel enthält folgende Themen:

[Standardkonfiguration](#) (siehe Seite 39)

[Andere mögliche Konfigurationen](#) (siehe Seite 40)

[Implementierungsmodell](#) (siehe Seite 40)

[Objektmodell](#) (siehe Seite 43)

[Referenzverknüpfungen zwischen verschiedenen Objekten](#) (siehe Seite 45)

[DTS-Szenario](#) (siehe Seite 46)

Standardkonfiguration

Bei einer Standardkonfiguration werden die DTS-Manager-Komponenten – TOS, NOS und SOS – auf einem Computer unter Windows 2003 zusammen mit einem DTS-Agenten installiert. Auf allen Computern, die in Datenübertragungsaktivitäten einbezogen sind, muss ein DTS Agent installiert sein.

Alle DTS-Funktionen wie Übertragungszeitpläne, Auflösung von Übertragungsrouten und Einleitung der eigentlichen Datenübertragungen werden auf demselben Computer ausgeführt. Ein einzelner TOS, NOS und SOS ist ausreichend, um diese Funktionen im gesamten Unternehmen durchzuführen.

Diese Art der Installation bietet die Möglichkeit, das DTS-Netzwerk zentral zu steuern.

Die folgenden Modelle können bei der Festlegung der optimalen Implementierung der DTS-Architektur für die gegebenen Anforderungen helfen:

- Implementierungsmodell
- Objektmodell

Andere mögliche Konfigurationen

Wenn nicht alle Funktionen der Manager-Komponenten auf einem einzelnen Computer benötigt werden oder aufgrund der Umstände eine Verteilung auf mehrere Computer vorteilhafter ist, können Sie die Manager-Komponenten auf verschiedenen Computern im Netzwerk installieren.

Wenn für einen Standort beispielsweise ein hohes Übertragungsaufkommen geplant ist, kann der TOS getrennt vom NOS und SOS auf einem separaten Computer installiert werden, um die Belastung eines einzelnen Computers zu verringern. Bei Bedarf können alle drei Server auf separaten Computern installiert werden.

Hinweis: Die tatsächlich angebotenen Konfigurationsoptionen können auch von der CA-Client-Lösung abhängen, die DTS installiert.

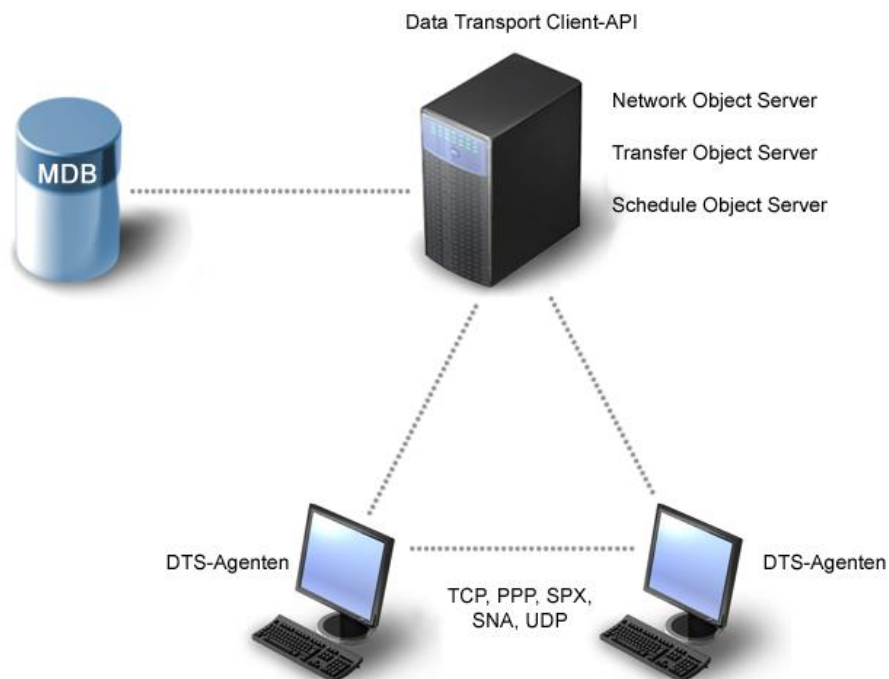
Implementierungsmodell

Im Implementierungsmodell wird gezeigt, wie das Produkt implementiert und wie der Dienst auf höherer Ebene bereitgestellt wird:

- Die Client-API teilt dem DTS Manager mit, was dieser tun soll.
- Der Manager ermittelt, wie dies geschehen soll, und weist den DTS Agenten anschließend entsprechend an.
- Der Agent führt diese Anweisungen aus und teilt dem Manager dann mit, dass der Task ausgeführt wurde.
- Der Manager teilt der Client-API mit, dass der Task ausgeführt wurde.

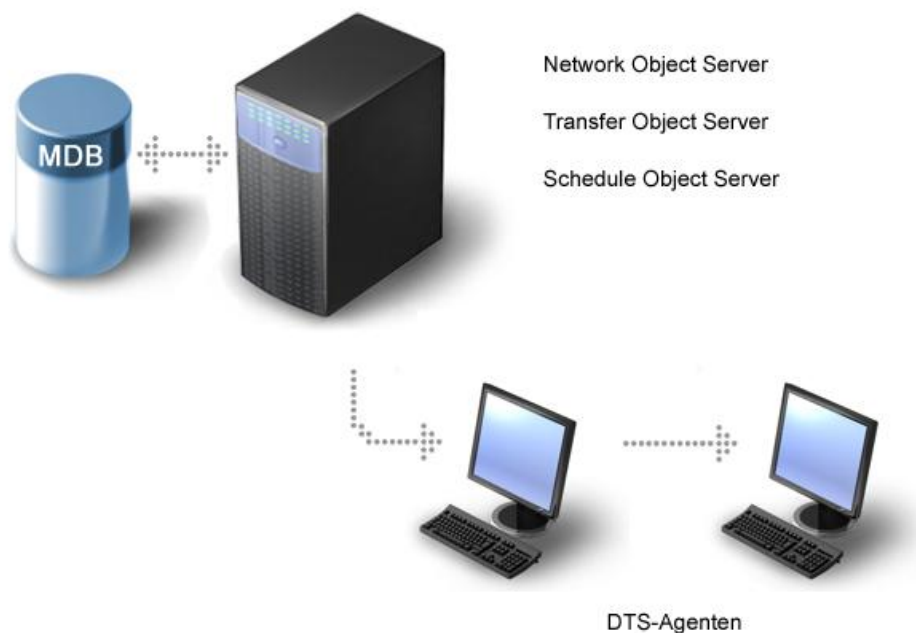
Die folgende Abbildung veranschaulicht, wie die DTS-Architektur sowohl Client/Server- als auch Manager/Agent-Methodologien implementiert. Gemeinsam garantieren diese Methodologien, dass die Implementierungsmöglichkeiten flexibel und skalierbar bleiben. In dieser Abbildung übernimmt der Manager die Server-Rolle der Client/Server-Lösung.

Benutzeranwendungen



Anwendungen, die DTS einsetzen wollen, rufen die in der DTS-Client-API enthaltenen Funktionen auf, die ihrerseits den DTS Manager anweisen, den angeforderten Task auszuführen. Der DTS Manager (DTM) umfasst drei separate Server (NOS, TOS und SOS). Jeder Servertyp hat eine besondere Rolle zu übernehmen, unabhängig davon, wie viele Instanzen implementiert sind.

Um besser verstehen zu können, wie die DTS-Komponenten zur Durchführung einer Datenübertragung zusammenarbeiten, betrachten Sie die folgende Abbildung:



Angenommen, ein Benutzer hat eine Übertragung für ein bestimmtes Datum und eine bestimmte Uhrzeit geplant. Wenn der festgelegte Zeitpunkt eintritt, erkennt der SOS, dass eine Übertragung erfolgen muss, und weist den TOS an, diese Übertragung auszuführen. Nach Empfang dieser Anforderung weist der TOS den auslösenden Agent an, die Übertragung der Daten auszuführen.

Um den Grad an Funktionalität, Management, Kontrolle und Flexibilität zu erreichen, den eine auftragskritische, unternehmensweite Datenübertragungslösung erfordert, verwendet DTS ein durchstrukturiertes Objektmodell. Durch das Erstellen von Objektinstanzen und das Einstellen von Eigenschaften und Aufrufmethoden können Sie die leistungsstarken Funktionen von DTS in vollem Umfang nutzen.

Objektmodell

Aus dem Objektmodell geht hervor, inwiefern sich DTS an den Objekten orientiert (OO). Objektorientiert bedeutet, dass Sie zur Nutzung der verfügbaren Dienste Objekte erstellen (anlegen) und diese (durch das Festlegen von Eigenschaften) sowie die mit diesen Objekten assoziierten Funktionsaufrufe (Methoden) konfigurieren. Das DTS-Objektmodell besteht aus einem Satz von Objektklassen, die gegenseitig aufeinander Bezug nehmen und miteinander interagieren. Für die Verwendung von DTS müssen folgende Schritte ausgeführt werden können:

- Herstellen einer Verbindung zu einem Objektserver
- Erstellen (Anlegen) von Objekten der entsprechenden Klassen
- Festlegen der Objekteigenschaften auf die geforderten Werte
- Aufrufen der Objektmethoden

Im Folgenden finden Sie eine kurze Beschreibung aller Klassen, die von DTS unterstützt werden:

DTContainer

Setzt DTS-Eigenschaften für eine Liste von DTMachine-Objekten außer Kraft. Mit DTContainers können Sie mehrere DTMachine-Objekte bei der Administration und Konfiguration der DTS-Netzwerktopologie als einzelne Entität behandeln. Dieses Objekt enthält alle DTS-Eigenschaften und Verweise auf ein oder mehrere DTMachine-Objekte.

DTDynamicContainer

Enthält die gleichen Eigenschaften wie die DTContainer-Klasse, weist jedoch eine zusätzliche Eigenschaft auf: eine Reihe von Adressen oder ein Subnetz, das die Mitglieder des Containers definiert. Alle Agenten, deren IP-Adresse in diesem Bereich liegt, werden Mitglieder des dynamischen Containers. Mit Hilfe von dynamischen Containern kann ein Benutzer Routen zwischen Computern und einem dynamischen Container erstellen.

DTFilter

Legt fest, wie die Daten gelesen oder geschrieben werden sollen und wie sie zu verarbeiten sind, bevor sie übertragen werden bzw. nachdem sie übertragen wurden. Beispielsweise können Filter für binäres Lesen, binäres Schreiben, Komprimierung, Dekomprimierung usw. verwendet werden.

DTInterface

Stellt eine Kommunikationsschnittstelle auf einem Computer dar.

DTLink

Stellt eine direkte DTS-Kommunikationsverknüpfung zwischen einem DTMachine-Objekt (oder DTContainer-Objekt) und einem anderen dar. Das Verknüpfungsobjekt erstellt bestimmte Routen innerhalb des DTS-Unternehmens.

Jeder Objektserver (Network, Transfer und Schedule Object Server) verwaltet Objekte bestimmter Klassen, die speziell auf die Funktion des Servers abgestimmt sind. Lokale Objekt-Repositorys (Datenbanken) speichern diese Objekte dauerhaft, für jeden Objektserver ist ein Repository vorhanden.

DTMachine

Definiert einen Computer im Unternehmen. Wenn der Computer über mehrere Kommunikationsschnittstellen verfügt, die DTS verwenden kann, verweist dieses Objekt auf ein oder mehrere DTInterface-Objekte.

DTMachineGroup

Stellt eine logische Gruppierung von Computern dar. Dieses Objekt verweist auf DTMachine-Objekte oder andere DTMachineGroup-Objekte.

DTSchedule

Legt fest, wann eine Datenübertragung erfolgen soll. Dieses Objekt verweist auf ein oder mehrere DTTransferGroup-Objekte. Dieses Objekt kann auch auf einen oder mehrere Kalender verweisen.

DTTransfer

Enthält eine Definition einer einzelnen Datenübertragung von einem Computer auf einen anderen. Unter anderem enthält dieses Objekt Verweise auf DTFilter-Objekte.

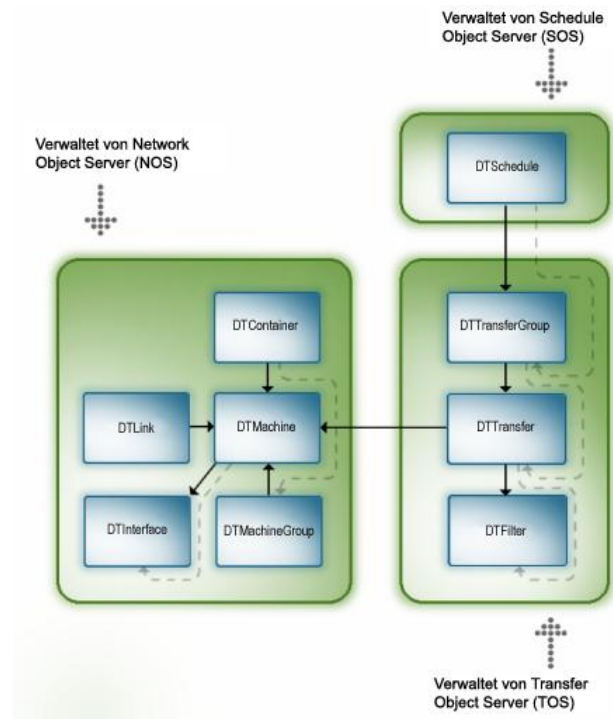
DTTransferGroup

Definiert eine Gruppe von Übertragungen, die gemeinsam gesteuert werden sollen und verweist auf ein oder mehrere DTTransfer-Objekte.

Hinweis: Der NOS verwendet die MDB als dauerhaften Objektspeicher. DTS nutzt die bereits in der MDB gespeicherten Netzwerkinformationen.

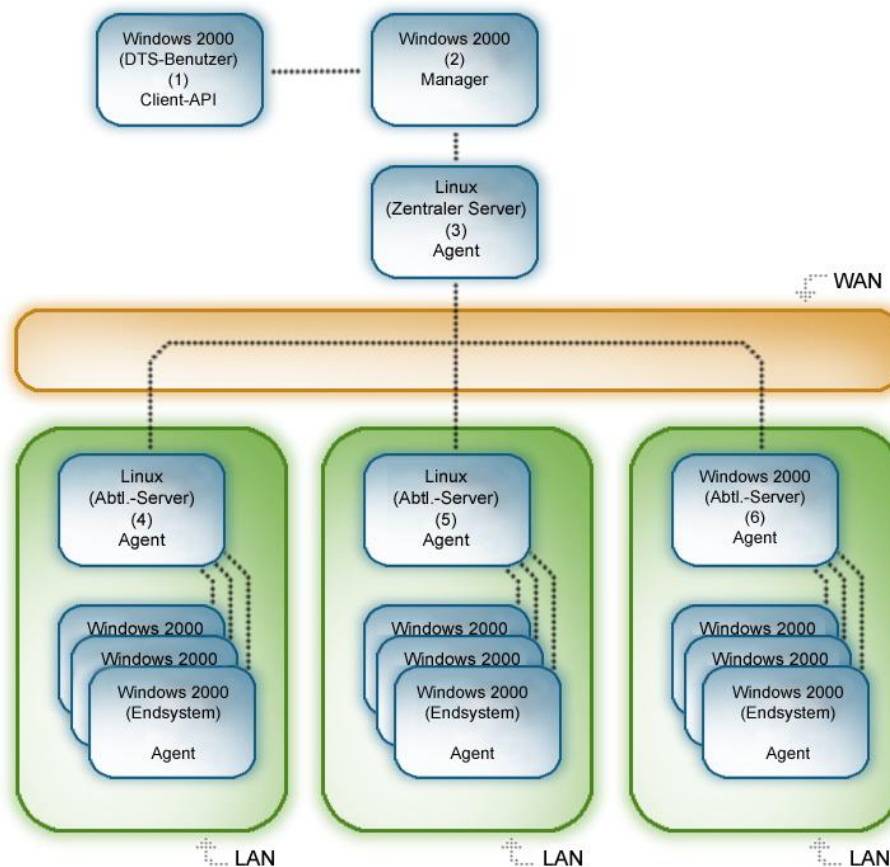
Referenzverknüpfungen zwischen verschiedenen Objekten

Die folgende Abbildung zeigt die Referenzverknüpfungen zwischen den verschiedenen Objektklassen. Außerdem ist dargestellt, welche Objektklassen von den einzelnen Servern verwaltet werden:



DTS-Szenario

Um das Verständnis der Auslösung einer Datenübertragung, der Verwendung des Objektmodells sowie der Rolle, die die einzelnen DTS-Komponenten spielen, zu erleichtern, wird ein typisches DTS-Szenario vorgestellt.



Angenommen, ein DTS-Administrator möchte an jedem Wochentag um 22 Uhr Datenübertragungen durchführen. Eine umfangreiche binäre Datendatei, die sich auf einem Linux-Server befindet, muss an zahlreiche Windows XP-Computer übertragen werden, die auf drei separate lokale Netzwerke (LANs) verteilt sind. Mit jedem LAN ist ein Abteilungsdateiserver verbunden. Der zentrale Server ist mit den LANs über ein WAN (Wide Area Network) mit relativ geringer Bandbreite verbunden. Auf den Abteilungsservern werden die Betriebssysteme Windows 2003 und Linux ausgeführt. Außerdem soll die Datendatei aufgrund der Vertraulichkeit ihres Inhalts während der Übertragung verschlüsselt werden.

Wie aus der vorherigen Abbildung hervorgeht, ist die Client-API nur auf dem DTS-Benutzer-Computer (1) installiert. Der DTS-Manager ist auf einem separaten Windows 2003-Computer (2) und der DTS-Agent auf dem zentralen Server (3), den Abteilungs-Servern (4, 5 und 6) sowie auf allen Endsystemen installiert, d. h. auf insgesamt 300 Endsystemen (unter der Annahme, dass jedes LAN 100 Endsysteme umfasst).

Auf dem Windows 2003-Manager-Computer (2) kann ebenfalls CA Common Services installiert sein. In diesem Fall ist er für alle Netzwerk- und Datenübertragungen sowie für das Planen von Tasks zuständig.

Datenübertragungsprobleme

Die Probleme, denen die heutige Geschäftswelt gegenübersteht, verlangen häufig nach Lösungen, die die Übertragung großer Mengen an kritischen Informationen (Daten) erfordern. Diese Informationen können von einem System ermittelt und an zahlreiche andere übertragen (verteilt) werden, oder sie können von mehreren Systemen ermittelt und an ein System gesendet (zentral erfasst) werden. Aufgrund der ständig wachsenden Zahl von Benutzern, die häufig durch große Entfernungen voneinander getrennt sind, ist die sichere und effektive Übertragung von Daten von einem Ort zu einem anderen ein schwer zu lösendes Problem.

Das Problem wird durch die Tatsache noch weiter erschwert, dass die Hardware eines Unternehmens häufig aus einer Ansammlung verschiedener Computer besteht, auf denen unterschiedliche Betriebssysteme ausgeführt werden und die mit Hilfe verschiedener Kommunikationsarten miteinander verbunden sind.

Der Task der zentralen Erfassung und Verteilung von Informationen kann Probleme bereiten, wenn die Daten über mehrere Plattformen hinweg und mit verschiedenen Protokollen in komplizierten Netzwerken verteilt werden müssen. Einige der im Zusammenhang mit Datenübertragungen immer wieder auftretenden Probleme sind:

Inkompatibilität zwischen Plattformen

Die Übertragung von Daten, die in unterschiedlichen Formaten auf verschiedenen Plattformen gespeichert sind, kann häufig ein Problem darstellen. Schwierigkeiten treten dann auf, wenn die Daten nicht von einer Plattform auf eine andere übertragen werden können oder wenn die Integrität der Daten aufgrund der Inkompatibilitäten zwischen den Plattformen verloren geht.

Netzwerkleistung

Die Verteilung umfangreicher Datenmengen über ein Netzwerk wirkt sich häufig auf andere Netzwerkbenutzer dadurch aus, dass das Netzwerk mit Daten überschwemmt wird.

Ineffizientes Routing

Das Unvermögen, die optimale Route zur Übertragung von Daten in einem großen und oftmals komplexen Netzwerk zu bestimmen, kann zu Ineffizienz und Zeitverlust führen.

Unzuverlässigkeit

Auftragskritische Daten müssen übertragen werden. Übertragungen müssen erfolgreich abgeschlossen werden, und die Benutzer müssen über erfolgreiche Übertragungen informiert werden. Datenübertragungsprogramme müssen also zuverlässig und transparent sein. Für die meisten trifft dies allerdings nicht zu.

Die Datenübertragungslösung

DTS ist eine umfassende Lösung mit folgenden Eigenschaften:

- Dank ihrer Integration in CA-Lösungen wie CA ITCM können Sie die CA-Client-Lösung einfach auspacken, installieren, und sofort damit arbeiten.
- Bietet plattformübergreifende Unterstützung. Dank seiner strukturierten und gleichzeitig praktischen Architektur ist die Portierung von DTS auf neue Plattformen und neue Betriebssysteme eine einfache Aufgabe. Der DTS-Agent wird von Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008 sowie von verschiedenen UNIX-Plattformen (einschließlich AIX, HP-UX und Solaris) unterstützt.

Hinweis: In CA ITCM laufen alle Komponenten von DTS-Manager (TOS, NOS und SOS) ausschließlich unter Windows Server 2003 und Windows Server 2008. Unter UNIX/Linux werden Manager nicht unterstützt. Weitere Informationen zu unterstützten Betriebsumgebungen finden Sie in der *Readme-Datei zu CA ITCM*.

- unterstützt mehrere Protokolle. Bei der DTS-Architektur liegt das gesamte Produkt oberhalb der Kommunikationsprotokollebene. Das Produkt ist also von keinem bestimmten Protokoll und von keiner besonderen Netzwerktechnologie abhängig. DTS lässt sich mühelos so erweitern, dass die Vorteile neuer Protokolle und Technologien genutzt werden können, sobald diese verfügbar sind.
- Ausführung über TCP, SNA, UDP, SPX und PPP. Um die Möglichkeiten Ihres Netzwerks optimal auszuschöpfen, nutzt DTS außerdem die Vorzüge der Broadcast- und Multicast-Netzwerktechnologien.

Hinweis: DTS unterstützt nicht die neueste Version des PPP-Kommunikationsprotokolls, PPPv6.

- Setzt integrierte CA Common Services wirksam ein. WorldView, Event Management, Workload Management, Agent-Technologie und die MDB sind Bestandteile von DTS und bieten eine einzigartige Übertragungslösung.
- erlaubt das Erstellen von Zeitplänen. Über die API werden einfache oder komplexe Zeitpläne erstellt und konfiguriert.
- enthält Funktionen zur Überwachung und Steuerung von Übertragungen. Der Fortschritt und Status sämtlicher in einem Unternehmen ablaufenden Datenübertragungen kann überwacht werden. Datenübertragungen können jederzeit abgebrochen oder ausgesetzt werden. Eine ausgesetzte (oder fehlgeschlagene) Übertragung kann zu einem späteren Zeitpunkt wiederaufgenommen werden.

- bietet Service-Management-Funktionen. Die Laufzeitparameter sämtlicher Service-Komponenten werden dynamisch geändert, die Service-Komponenten überwacht und Protokolldateien eingesehen.
- kann auf Wunsch zentralisiert oder verteilt werden. Es ist sogar eine Kombination aus beidem möglich.
- Verwendet Client/Server-Technologie, um eine echte netzwerkbasierte Schnittstelle bereitzustellen. Mit DTS können Sie beispielsweise auch Daten zwischen beliebigen Computern Ihres Unternehmens übertragen.
- Realisiert Sicherheit auf vielen Ebenen. Benutzer- und Kennwortauthentifizierung können auf Client-, Server-, Manager- und Agenten-Ebene aktiviert werden. Daten können auch mit Hilfe einer Vielzahl an Algorithmen verschlüsselt werden.
- Enthält eine Optimierungs-Engine, mit der sichergestellt wird, dass DTS Ihr Netzwerk optimal ausnutzt. DTS ermittelt die optimalen Routen für Ihr Enterprise, löst Übertragungseinstellungen auf und sucht aufgrund der zu übertragenden Datenangaben das beste Übertragungsverfahren aus.
- Verfügt über eine durch den Benutzer erweiterbare Architektur. DTS bietet ein voll funktionsfähiges Software Development Kit (SDK) und die Möglichkeit, eigene Agenten-Filter zu definieren. Durch die Kombination dieser Funktionen können Sie die Erweiterung von DTS optimal steuern.

Lösen des Problems

Bei der Vorbereitung einer Datenübertragung sollten Sie genau überlegen, was Sie erreichen möchten: Welche Daten müssen übertragen werden, wohin müssen diese Daten übertragen werden, und wie und wann soll die Übertragung stattfinden? Wenn Sie diese Fragen beantwortet haben, können Sie feststellen, welche DTS-Objekte benötigt werden, um diese Anforderungen zu erfüllen.

Dieser Vorgang ist, insgesamt betrachtet, relativ einfach. Als Erstes müssen Sie das DTS-Netzwerk konfigurieren bzw. ein Modell davon erstellen. Anschließend müssen Sie sämtliche erforderlichen Übertragungen, Zeitpläne usw. erstellen.

Erstellen eines Netzwerkmodells

Das Erstellen eines Netzwerkmodells umfasst das Anlegen von logischen Verbindungen zwischen den Netzwerkcomputern, um die gewünschten Datenübertragungsanforderungen zu erfüllen. Standardmäßig wird davon ausgegangen, wenn DTS installiert ist, dass sämtliche Computer direkt miteinander verbunden sind. Ihre erste Aufgabe besteht daher darin, ein Modell des Netzwerks zu erstellen, das Ihre logischen Erfordernisse erfüllt.

Betrachten Sie das Beispielszenario. Standardmäßig hat, sofern dies Data Transport betrifft, der zentrale Server eine direkte Verbindung zu allen Endsystemen. Wenn Sie jedoch DTS anweisen, die Datendatei vom zentralen Server auf alle Endsysteme zu übertragen, würde das Programm standardmäßig eine Fanout-Übertragung durchführen. Die Optimierungs-Engine erkennt, dass die Quelldatendatei für sämtliche Übertragungen identisch ist und die Daten daher nur einmal gelesen werden müssen.

Mit DTS können Sie eine einfache Netzwerkkonfiguration durchführen (ein Modell für das Data Transport-Netzwerk erstellen) und einige Objekteigenschaften anpassen, um es DTS zu ermöglichen, einige Vorteile seiner leistungsfähigen Übertragungstechnologie zu nutzen. Die Data Transport-Netzwerkanforderungen können mit Hilfe von WorldView eingestellt werden.

Sie möchten DTS davon abhalten, Daten direkt vom zentralen Server an die Endsysteme zu senden, stattdessen sollen die Daten über die Abteilungsserver übertragen werden. Dafür müssen Sie eine Route vom zentralen Server über die Abteilungsserver zu den Endsystemen festlegen. Sie können dies erreichen, indem Sie Data Transport-Verknüpfungen zum Netzwerkmodell hinzufügen.

Zunächst werden drei Verknüpfungen zwischen dem zentralen Server und jedem der Abteilungsserver hergestellt. Anschließend erstellen Sie drei Data Transport-Computercontainerobjekte, d.h. eins für jedes LAN. Nehmen Sie sämtliche Computer, die mit den LANs verbunden sind (mit Ausnahme der Abteilungsserver), in die jeweils relevanten Container auf.

Als Nächstes müssen Sie von jedem der Abteilungsserver Verknüpfungen zu den ihnen entsprechenden Computercontainerobjekten erstellen. Abschließend soll DTS bei der Übertragung von Daten von den Abteilungsservern zu den Endsystemen auf den lokalen LANs die Vorteile des Punkt-zu-Viele-Übertragungsverfahrens nutzen. Da außerdem Daten an Computer übertragen werden, die mit demselben IP-Subnetz verbunden sind, verwendet DTS das Broadcast-Protokoll (BCAST).

Bei DTS gibt es mehrere Möglichkeiten, um dasselbe Ergebnis zu erreichen. Es ist jedoch einfacher, die Punkt-zu-Viele-Protokolleigenschaft der Verknüpfung "Abteilungsserver an Container" auf BCAST und die Punkt-zu-Viele-Netzwerkadresse auf die für das Subnetz entsprechende Broadcast-Adresse einzustellen. Diese Einstellungen können Sie in WorldView vornehmen, indem Sie mit der rechten Maustaste auf den Link klicken und im Kontextmenü "DTS-Details öffnen" auswählen.

Mit der Option "DTS-Details öffnen" können Sie die folgenden Eigenschaften ändern:

- Maximale Paketgröße
- Drosselungsfaktor
- Punkt-zu-Punkt-Protokoll und Parameter
- Fanout-Protokoll und Parameter
- Punkt-zu-Viele-Protokoll und Parameter

Maximale Paketgröße

DTS überträgt Daten in kleinen Blöcken, die "Pakete" genannt werden. Die Größe des Pakets beeinflusst viele Faktoren, unter anderem:

Allgemeine Übertragungsleistung

Je größer das Paket, desto schneller die Übertragung.

Vom Agenten verwendete Systemressourcen

Je größer das Paket, desto mehr Arbeitsspeicher wird vom Agenten verwendet (da er jederzeit während der Übertragung mindestens ein Datenpaket im Arbeitsspeicher hat).

Checkpoint-Neustart

Jedes Paket wird nach der Übertragung als Teil der automatischen Checkpoint-Neustart-Funktion gekennzeichnet. Tritt während des Übertragungsvorgangs ein Fehler auf, kann DTS die Übertragung vom letzten erfolgreich gesendeten Paket her neu starten.

System- bzw. Netzwerkgeschwindigkeit

Dateiübertragungen zwischen Agenten auf langsameren Rechnern oder in langsameren Netzwerken werden möglicherweise angehalten oder mit der Meldung "Verbindung fehlgeschlagen *Adresse|Hostname*" ergebnislos abgebrochen. Diese Bedingung kann durch das Überschreiten eines Zeitlimits bei der Verarbeitung großer Datenpakete ausgelöst werden. In diesem Fall sollten Sie die maximale Paketgröße für die Datenübertragung an die Leistungsfähigkeit des langsamsten Systems anpassen.

Drosselungsfaktor

Mit der Drosselung kann die bei der Durchführung von Datenübertragungen verwendete Netzwerkbandbreite reguliert werden, indem ein Verzögerungsintervall zwischen Paketsendevorgängen festgelegt wird. Die Drosselungsfaktoreigenschaft legt den Wert der Verzögerung fest. Zulässige Werte liegen zwischen 0 und 100. Die Standardanzahl beträgt 0. Jede Erhöhung des Drosselungsfaktors verlängert das Verzögerungsintervall um 50 Millisekunden. Beispielsweise steht ein Drosselungsfaktorwert von 20 für ein Verzögerungsintervall von einer Sekunde zwischen den Paketsendevorgängen.

Ändern von DTS-Objekteigenschaften

Wenn DTS und CA Common Services installiert sind, wird der Menübefehl "DTS-Details öffnen" dem WorldView-Kontextmenü für alle verwalteten Objekte hinzugefügt. Mit dem Befehl "DTS-Details öffnen" können Sie schreibgeschützte Eigenschaften anzeigen und die DTS-Eigenschaften ändern, die mit dem Objekt verknüpft sind, auf das Sie mit der rechten Maustaste geklickt haben. Bei dem Objekt kann es sich um eine Verknüpfung, eine Schnittstelle, einen Computer oder einen Computercontainer handeln.

Ändern von einzelnen Objekteigenschaften

Wenn Sie "DTS-Detail öffnen" auswählen, wird das Notizbuch für Objektdetails angezeigt, in dem Sie folgende Eigenschaften ändern können:

- Maximale Paketgröße
- Drosselungsfaktor
- Punkt-zu-Punkt
- Fanout
- Punkt-zu-Viele

Hinweis: Namen-, UUID-, Klassen-, Bezeichnungs-, Beschreibungs- und Adresseneigenschaften sind schreibgeschützte Eigenschaften (nur Informationen).

Administratoren steuern durch Ändern dieser Eigenschaften die Ausführung der Datenübertragung von DTS und konfigurieren die DTS-Netzwerktopologie für optimale Leistungsfähigkeit.

/Hinweis: Wenn kein Eigenschaftswert angegeben wird, ist die Eigenschaft nicht definiert, und es wird der Standardwert verwendet.

Erstellen von Übertragungsobjekten

Wenn Sie eine Binärdatei während der Übertragung verschlüsseln möchten, müssen Sie folgende Vorgänge ausführen: Einlesen der Daten mit einem binären Filter oder Textfilter, Anwenden eines Verschlüsselungsfilters, Übertragen der Daten, Anwenden eines Entschlüsselungsfilters und Ausgeben der Daten mit Hilfe eines binären Filters oder eines Textfilters. Sie können im Transfer Object Repository eigene Filterobjekte erstellen; zum Lieferumfang von DTS gehören jedoch zur Vereinfachung häufig eingesetzter Datenverarbeitungsoperationen viele vordefinierte Filterobjekte, die Sie anstelle der selbst zu erstellenden Filterobjekte verwenden können.

Als Nächstes müssen Sie Übertragungsobjekte erstellen, die die Datendateiübertragung vom Solaris-Zentralserver auf die einzelnen Endsysteme definieren. Sie müssen für jedes Endsystem genau ein Übertragungsobjekt erstellen und konfigurieren. Diese Übertragungsobjekte sollten bis auf den Namen des Empfängercomputers identisch sein. Jedes Übertragungsobjekt muss außerdem auf die passenden Filterobjekte für binäre Lese-, Verschlüsselungs-, Entschlüsselungs- und binäre Schreibvorgänge verweisen.

Sie können ein Übertragungsgruppenobjekt (einen sogenannten Übertragungsjob) erstellen und diesem sämtliche zuvor erstellten Übertragungsobjekte hinzufügen. Erstellen Sie als Nächstes einen Kalender, in dem Sie Übertragungen für jeden Wochentag aktivieren.

Danach erstellen Sie ein Zeitplanobjekt und stellen seine Zeiteigenschaft auf 22:00 Uhr ein. Erstellen Sie außerdem einen Verweis auf das vorher erstellte Übertragungsgruppenobjekt und den Kalender, und aktivieren Sie das Zeitplanobjekt.

DTS-Benutzer oder -Administratoren können alle vorher genannten Aufgaben zum Erstellen, Planen und Aktivieren der Übertragung mit Hilfe der folgenden Mittel ausführen:

- DTS-Befehl "dtscli".
- DTS-Client-API.

Hinweis: Detaillierte Informationen finden Sie im *Referenzhandbuch für DTSCLI-Befehle*.

Weitere Informationen:

[Filter](#) (siehe Seite 35)

[DTS-Client-API](#) (siehe Seite 37)

[dtscli \(Befehl\)](#) (siehe Seite 13)

Kapitel 4: Konfigurieren des Data Transport Service

DTS-Agenten und -Manager werden in CA ITCM mit Konfigurationsrichtlinien verwaltet. Eine Konfigurationsrichtlinie ist eine Reihe von Parametern, die das Verhalten einer bestimmten Komponente bestimmen. Konfigurationsrichtlinien können in CA ITCM im DSM-Explorer über die Knoten "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Standardcomputerrichtlinie", "DSM" angezeigt und geändert werden.

Dieses Kapitel enthält folgende Themen:

[Anzeigen der Konfigurationsrichtlinien](#) (siehe Seite 55)

[Ändern der Konfigurationsrichtlinien](#) (siehe Seite 56)

Anzeigen der Konfigurationsrichtlinien

Wichtig! Die Laufzeitparameter für CA ITCM-DTS-Agenten und -Manager können nicht über die Dialogfelder der WorldView-Komponente von CA Common Services konfiguriert werden, da dies die Richtlinie verletzen würde, die im DSM-Explorer eingerichtet wurde. Die Dialogfelder des DTS WorldView-Admin-Clients sind ausschließlich für die Konfiguration von Komponenten von Data Transport Service r1, r2 und r3 bestimmt.

Die Einstellungen der Konfigurationsrichtlinien für die DTS-Komponenten befinden sich in der Richtliniengruppe "Data Transport Service (DTS)" unter dem Knoten "Standardcomputerrichtlinie", "DSM" und werden im Fensterbereich "Data Transport Service (DTS)" angezeigt.

Diese Einstellungen werden zu den verschiedenen Notizbuchseiten und -dialogfeldern im DTS WorldView-Admin-Client weitergeleitet, auf den über die WorldView-Komponente von CA Common Services zugegriffen werden kann.

Die Richtliniengruppe "Data Transport Service (DTS)" enthält die folgenden Richtliniengruppenordner:

- Audit
- Data Browser Agent Plugin
- Data Transport Agent Plugin
- Makro
- Network Object Server
- Schedule Object Server
- Transfer Object Server

Wenn Sie zum Beispiel zweimal auf den Knoten "Data Transport Agent Plugin" klicken, werden im Fensterbereich "Data Transport Agent Plugin" die einzelnen Richtlinien dieser Richtliniengruppe angezeigt, z. B. Agent-Audit-Modus, Gleichzeitige Ausführung, Diskreter Modus, Heartbeat-Zeitlimit usw.

Weitere Informationen:

[Netzwerk-Administration](#) (siehe Seite 11)

Ändern der Konfigurationsrichtlinien

Sie können die DTS-Konfigurationsrichtlinien ändern.

So ändern Sie eine Richtlinieneinstellung:

1. Doppelklicken Sie auf die entsprechende Richtlinie, z. B. "Diskreter Modus".
Das Dialogfeld "Eigenschaften von Einstellung" wird angezeigt, in dem Sie den Wert ändern können.
2. Ändern Sie im Feld "Wert" den Wert nach Bedarf, und klicken Sie auf "OK".

Hinweis: Weitere Informationen zu den DTS-Konfigurationsrichtlinien und dem Umgang damit - Versiegeln und Aufheben der Versiegelung von Richtlinien, Ändern von Richtlinien, Erstellen neuer Richtlinien usw. - finden Sie im Abschnitt "Konfigurationsrichtlinie" in der *DSM-Explorer-Hilfe*.

Weitere Informationen:

[Self Discovery](#) (siehe Seite 14)

[Netzwerk-Administration](#) (siehe Seite 11)

Kapitel 5: Anpassen des Data Transport Service

Sie können Ihre DTS-Installation auf folgende Weise anpassen:

- Erstellen von angepassten Netzwerktopologien speziell für Ihr Enterprise
- Anpassen von Meldungen und Audit-Ebenen
- Verwenden von Kalendern zum Starten und Beenden von auf zeitbasiertem Routing basierenden Übertragungen

Dieses Kapitel enthält folgende Themen:

[Erstellen einer Netzwerktopologie](#) (siehe Seite 57)

[Ändern der Audit-Ebenen](#) (siehe Seite 59)

[Anpassen von Audit-Meldungen](#) (siehe Seite 62)

Erstellen einer Netzwerktopologie

Das Framework für ein Data Transport Service-Netzwerk wird erstellt, wenn die Prozesse Install Network Business Process Views und Data Transport Audio Discovery ausgeführt wurden. Drei Business Process Views sind enthalten: DTS-Manager-Konfiguration, DTS-Agenten-Konfiguration und DTS-Administration. Diese Anzeigen enthalten Grafiken und Beschreibungen zu den Data Transport-Objekten (DTS-Manager und -Agenten) und können über die WorldView-2D-Karten und -3D-Karten für die Objektverwaltung ausgewählt werden.

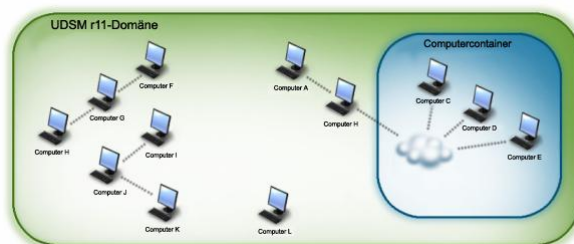
Sie können die Computer in Ihrem Netzwerk, die Netzwerktopologie für die Rechner in diesem Netzwerk und die Kommunikationsrouten für die Datenübertragung zwischen den Computern festlegen. Indem Sie eine Netzwerktopologie für Ihr Data Transport Network herstellen, können Sie eine strenge hierarchische Netzwerkstruktur definieren, in der die Routen für die Übertragung zwischen den Rechnern Ihres Netzwerks vom Data Transport Service bestimmt werden.

Durch die definierten Computer- und Netzwerkeigenschaften, die mit Hilfe der DTS-Admin-Client-Schnittstelle festgelegt und in der MDB gespeichert sind, werden die hierarchischen und netzwerkbezogenen Beziehungen zwischen den Rechnern Ihres Netzwerks hergestellt. Diese Beziehungen erzwingen die für den Abschluss der Übertragungen durch die Rechner und zwischen den Rechnern Ihres Netzwerks verwendete Route.

Rechner- und Netzwerkeigenschaften können auf Rechner-, Schnittstellen-, Computercontainer- und Verknüpfungsebene festgelegt werden. Wenn verschiedene Gruppen von Eigenschaften beim Auflösen einer Route über das Netzwerk gefunden werden, erhalten die Rechner- und Netzwerkeigenschaften den Vorrang, die am meisten Auswirkung auf die Übertragung haben. Sobald diese Eigenschaften bestimmt sind, übernimmt die Übertragung diese Eigenschaftenwerte, und die Route wird aufgelöst.

Bei Rechnern, die Bestandteil Ihrer Netzwerktopologie sind und die nicht in einer Hierarchie definiert sind, die aus einer oder mehreren Verknüpfungen besteht, wird von einer Punkt-zu-Punkt-Verbindung mit allen anderen Rechnern in Ihrem Netzwerk ausgegangen.

Gehen Sie von folgender Domänen-Netzwerktopologie aus:



In diesem Beispiel wird eine Netzwerktopologie zwischen den Rechnern einer CA ITCM-Domäne definiert. Rechnerhierarchien sind zusammen mit Rechnern, die kein Teil einer definierten Hierarchie sind, in derselben Netzwerktopologie vorhanden.

Unter Berücksichtigung der zwischen den Rechnern aufgrund der definierten Netzwerktopologie hergestellten Beziehungen kann folgende Aussage getroffen werden:

- Computer A und B sowie die Computer des Computercontainers (C, D und E) weisen eine Hierarchie auf.
- Computer F, G und H sowie Computer I, J und K sind ebenfalls Beispiele für separat hergestellte Hierarchien.
- Computer C, D und E sind Mitglieder eines Computercontainers. Wenn sich diese Computer auf der Containerebene befinden, können Sie allgemeine Übertragungseigenschaften für diese Computer definieren und diese auf alle Computer im Container anwenden. Definierte Computercontainereigenschaften haben Vorrang über die einzelnen Computereigenschaften.

- Zwischen den Computern C, D und E sowie zwischen B und G sind keine definierten Routen vorhanden. Wenn Sie eine Übertragung zwischen diesen Computern initiieren, wird von einer Punkt-zu-Punkt-TCP/IP-Verbindung ausgegangen.
- Eine Route vom Computer A zum Computer E wird in zwei Routen aufgelöst: Eine vom Computer A zum Computer B und eine zweite vom Computer B zum Computer E.

Hinweis: Weitere Informationen finden Sie in der CA WorldView-Dokumentation für Business Process Views.

Ändern der Audit-Ebenen

Sie können Auditing beim DTS-Agenten, TOS, NOS oder SOS aktivieren oder deaktivieren, indem Sie die entsprechende Konfigurationsrichtlinie für das Auditing im DSM-Explorer festlegen. Wenn Sie Auditing aktivieren, werden Auditing-Meldungen von der angegebenen Komponente ausgegeben, sobald die auslösenden Ereignisse auftreten. Wenn Sie Auditing deaktivieren, werden keine Auditing-Meldungen von der angegebenen Komponente ausgegeben, sobald die auslösenden Ereignisse auftreten. Die Auditing-Meldungen (unabhängig davon, ob sie benutzerdefiniert sind oder nicht) werden zwar ignoriert, jedoch nicht gelöscht. Die Meldungen können wieder aktiviert werden, sobald dies erforderlich ist.

Hinweis: Vor dem Ändern einer Richtlinie muss zuerst die Versiegelung aufgehoben werden. Weitere Informationen finden Sie im Abschnitt "Konfigurationsrichtlinie" in der *DSM-Explorer-Hilfe*.

Weitere Informationen:

[Auditing](#) (siehe Seite 22)

Aktivieren/Deaktivieren von Agent-Auditing

Sie können Auditing beim DTS-Agenten aktivieren oder deaktivieren, indem Sie die entsprechende Konfigurationsrichtlinie für das Auditing im DSM-Explorer festlegen.

So aktivieren bzw. deaktivieren Sie das Agent-Auditing:

1. Navigieren Sie zum Unterknoten "Data Transport Service (DTS)" unter "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Standardcomputerrichtlinie", "DSM".
2. Klicken Sie auf den Unterknoten der Richtliniengruppe "Data Transport Agent Plugin".

Alle Richtlinien für den DTS-Agenten werden im Data Transport Agent Plugin-Fenster angezeigt (rechter Fensterbereich).

3. Doppelklicken Sie in diesem Fensterbereich auf die Richtlinie "Audit-Modus".
Das Dialogfeld "Eigenschaften von Einstellung" wird angezeigt.
4. Setzen Sie das Feld "Wert" gegebenenfalls auf "True" bzw. "False". (Der Standardwert ist "True".)
5. Klicken Sie auf "OK".

Die Agent-Auditing-Funktion ist aktiviert bzw. deaktiviert.

Aktivieren/Deaktivieren von TOS-Auditing

Sie können Auditing für den TOS aktivieren oder deaktivieren, indem Sie die entsprechende Konfigurationsrichtlinie für das Auditing im DSM-Explorer festlegen.

So aktivieren bzw. deaktivieren Sie TOS-Auditing:

1. Navigieren Sie zum Unterknoten "Data Transport Service (DTS)" unter "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Standardcomputerrichtlinie", "DSM".
2. Klicken Sie auf den Unterknoten der Richtliniengruppe "Transfer Object Server".
Alle Richtlinien für den Transfer Object Server werden im Transfer Object Server-Fenster angezeigt.
3. Doppelklicken Sie in diesem Fenster auf die Richtlinie "Manager Auditing".
Das Dialogfeld "Eigenschaften von Einstellung" wird angezeigt.

4. Setzen Sie das Feld "Wert" für die vom Manager (DTS Transfer Object Server) verwendete Auditing-Detailebene. Folgende Werte sind gültig:

0 - Deaktiviert

Gibt keine Audit-Meldungen an, d.h. Auditing ist deaktiviert.

1 - Minimal

Gibt nur Server-Meldungen an.

2 - Standard

Gibt Server-, Übertragungsjob- und Übertragungsfehlermeldungen an.

3 - Erweitert

Gibt alle Audit-Meldungen an.

Standard: 1

5. Klicken Sie auf "OK".

Die TOS-Auditing-Funktion ist aktiviert bzw. deaktiviert.

Aktivieren/Deaktivieren von NOS-Auditing

Sie können Auditing für den NOS aktivieren oder deaktivieren, indem Sie die entsprechende Konfigurationsrichtlinie für das Auditing im DSM-Explorer festlegen.

So aktivieren bzw. deaktivieren Sie NOS-Auditing:

1. Navigieren Sie zum Unterknoten "Data Transport Service (DTS)" unter "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Standardcomputerrichtlinie", "DSM".
2. Klicken Sie auf den Unterknoten der Richtliniengruppe "Network Object Server".
Alle Richtlinien für den Network Object Server werden im Network Object Server-Fensterbereich angezeigt.
3. Doppelklicken Sie in diesem Fensterbereich auf die Richtlinie "Manager auditing mode".
Das Dialogfeld "Eigenschaften von Einstellung" wird angezeigt.
4. Setzen Sie das Feld "Wert" gegebenenfalls auf "True" bzw. "False". (Der Standardwert ist "True".)
5. Klicken Sie auf "OK".
Die NOS-Auditing-Funktion ist aktiviert bzw. deaktiviert.

Aktivieren/Deaktivieren von SOS-Auditing

Sie können Auditing für den SOS aktivieren oder deaktivieren, indem Sie die entsprechende Konfigurationsrichtlinie für das Auditing im DSM-Explorer festlegen.

So aktivieren bzw. deaktivieren Sie SOS-Auditing:

1. Navigieren Sie zum Unterknoten "Data Transport Service (DTS)" unter "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Standardcomputerrichtlinie", "DSM".
2. Klicken Sie auf den Unterknoten der Richtliniengruppe "Schedule Object Server".
Alle Richtlinien für den Schedule Object Server werden im Schedule Object Server-Fenster angezeigt.
3. Doppelklicken Sie in diesem Fensterbereich auf die Richtlinie "Manager auditing mode".
Das Dialogfeld "Eigenschaften von Einstellung" wird angezeigt.
4. Setzen Sie das Feld "Wert" gegebenenfalls auf "True" bzw. "False". (Der Standardwert ist "True".)
5. Klicken Sie auf "OK".
Die SOS-Auditing-Funktion ist aktiviert bzw. deaktiviert.

Anpassen von Audit-Meldungen

Die Meldungen für häufig eintretende Ereignisse, wie das Fehlschlagen des DTS-Agenten bzw. des Transfer Object Servers oder den Abbruch eines Übertragungsjobs, können von Data Transport Service-Administratoren angepasst werden. Dabei wird die (Standard-)Meldung, die von Data Transport Service normalerweise bei Vorliegen der entsprechenden Bedingungen ausgegeben wird, durch die angepasste Meldung ersetzt.

Wenn beispielsweise vor einer solchen Anpassung der Network Object Server während des Normalbetriebs fehlschlägt, sendet Data Transport Service das Ereignis an das Common Application Framework (CAF), das die Standardmeldung "Network Object Server-Fehler" an die Network Object Server-Protokolldatei und die Konsole weiterleitet. Wenn Sie jedoch die Richtlinie "NOS_FAILURE" im DSM-Explorer in der Richtliniengruppe "Audit" mit einem *Audit-Token* versehen, sendet Data Transport Service anstelle der Standardmeldung Ihre benutzerdefinierte Meldung an die Konsole.

So können Administratoren mit Hilfe benutzerspezifischer Meldungen Fehler flexibler handhaben. Wenn sich beispielsweise der Network Object Server auf einem Computer an Ihrem Standort befindet, von dem bekannt ist, dass er gelegentlich abstürzt und neu gestartet werden muss, könnten Sie dies zum Text der angepassten Meldung hinzufügen.

Sie können nur Meldungen anpassen, die als Audit-Token im DSM-Explorer zur Verfügung stehen. Die Audit-Token werden auf Übertragungen, Übertragungsjobs sowie auf die Server und die Agenten angewendet.

Hinweis: Audit-Meldungen und Makros sind im Lieferumfang von Data Transport Service r2 und r3 inbegriffen. Darüber hinaus ist eine Anpassung von anderen von Data Transport Service ausgegebenen Meldungen, einschließlich Meldungen zu Protokollen, Filtern, Verschlüsselung oder dem bei der Übertragung verwendeten Betriebssystem, *nicht möglich*.

Weitere Informationen:

[Auditing](#) (siehe Seite 22)

Audit-Protokolldateien

In CA ITCM verwenden sowohl die Manager als auch die Agenten die Common Event-Komponente. Das bedeutet, dass es die Protokolldatei "dtaaudit.log" im Gegensatz zu früheren Versionen nicht mehr gibt. Zwar werden alle Auditing-Meldungen an das Windows-Anwendungsprotokoll oder eine angegebene Datei weitergeleitet, gesteuert wird dieses Verhalten jedoch von der CA ITCM-Ereigniskomponente.

Audit-Token

Jedes Audit-Token definiert eine Meldung für die CA ITCM-Ereigniskomponente, die beim Auftreten eines bestimmten Ereignisses, z. B. beim Start oder bei der Beendigung eines Übertragungsjobs, an das Anwendungsprotokoll und an die Agent-Auditing-Protokolldatei übertragen wird. Sie können die Meldungen (den sogenannten Audit-Wert) für die einzelnen Token so anpassen, dass sie freien Text und Makros enthalten, die bei der Ausgabe des Tokens, d. h. bei der Ausgabe der Meldung durch den Data Transport-Server oder -Agenten, erweitert werden.

Die folgenden Audit-Token stellen die Ereignisse dar, für die Sie die Meldungen des DTS Agenten anpassen können. Als Audit-Wert werden ggf. Makros und freier Text eingesetzt, die Sie für diese einzelnen Ereignisse angeben können.

DTA_ABORT=\${DT} \${TT} Übertragung von \${XF} nach \${XT}abgebrochen.
 DTA_COMPLETE=\${DT} \${TT} Übertragung von \${XF} nach \${XT} abgeschlossen.
 DTA_FAIL=\${DT} \${TT} Übertragung von \${XF} nach \${XT} fehlgeschlagen;
 Fehlermeldung=\${XX}.
 DTA_START=\${DT} \${TT} Übertragung von \${XF} nach \${XT} gestartet.
 DTA_SUSPEND=\${DT} \${TT} Übertragung von \${XF} nach \${XT} ausgesetzt.
 DTA_RESUME=\${DT} \${TT} Übertragung von \${XF} nach \${XT} wiederaufgenommen.
 AUDIT_START=\${DT} \${TT} Audit-Datei gestartet.
 AUDIT_END=\${DT} \${TT} Audit-Datei beendet.

Die erste Gruppe von Audit-Token (DTA_ABORT ... DTA_RESUME) wird ausgegeben, wenn eine Übertragung, die diesen Agenten als Initiator oder Responder angibt, abgebrochen, beendet, gestartet, ausgesetzt bzw. nach dem Aussetzen wiederaufgenommen wird oder fehlschlägt.

Diese Meldungen stellen auf die Übertragung bezogene Informationen zum Initiieren des DTS-Agenten bereit. Dies kann sehr hilfreich sein, da übertragungsbezogene Meldungen vom TOS nicht auf dem Agentencomputer angezeigt werden, es sei denn, der TOS und der Agent befinden sich auf demselben Computer.

Die letzten beiden Audit-Token (AUDIT_START und AUDIT_END) werden ausgegeben, wenn Auditing aktiviert oder deaktiviert wird.

Die Makros $\{DT\}$ und $\{TT\}$, die in jeder oben aufgeführten Audit-Meldung verwendet werden, stellen die Kurzformen für $\{DateStandard\}$ und $\{TimeStandard\}$ dar. Diese Makros zeigen Datum und Uhrzeit im Standardformat der C-Bibliothek für diesen DTS-Agentencomputer an.

Anpassen von Audit-Tokens

Sie können Audit-Tokens in CA ITCM anpassen.

So passen Sie den Wert eines der aufgeführten Audit-Tokens an:

1. Navigieren Sie im DSM-Explorer unter "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Standardcomputerrichtlinie" im DSM-Knoten zum Unterknoten "Data Transport Service (DTS)".

2. Klicken Sie auf den Unterknoten der Richtliniengruppe "Audit".

Alle Richtlinien für das DTS-Auditing werden im Audit-Fenster angezeigt (rechter Fensterbereich).

3. Doppelklicken Sie auf die entsprechende Richtlinie, z. B. "DTA_ABORT".

Das Dialogfeld "Eigenschaften von Einstellung" wird angezeigt.

4. Bearbeiten Sie den Standardtext für das mit der ausgewählten Richtlinie verknüpfte Audit-Token.

5. Klicken Sie auf "OK".

Das ausgewählte Audit-Token wird angepasst.

Der vordefinierte Audit-Wert für die übertragungsbezogenen Audit-Tokens (DTA_ABORT ... DTA_RESUME) enthält Folgendes:

- Einen kurzen, freien Text ("Übertragung von...bis...Ereignis"), der den Verlauf der Übertragung erläutert, z. B. Start, Abbruch oder Fehlschlagen der Übertragung.
- Das Makro {XF} - die Kurzform für {TransferFrom} - gibt den sendenden Computer in der Übertragung an.
- Das Makro {XT} - die Kurzform für {TransferTo} - gibt den empfangenden Computer in der Übertragung an.

Die Meldung DTA_FAIL enthält den folgenden, zusätzlichen Satz:

... Fehlermeldung=\${XX}.

Das Makro {XX} - die Kurzform für {TransferExit} - gibt die Ursache für das Fehlschlagen der Übertragung an. Dieses Makro zeigt die Standardmeldungsnummer und den Text für den Fehler an.

Der vordefinierte Audit-Wert für die Audit-Token AUDIT_START und AUDIT_END enthält Folgendes:

- Einen kurzen freien Text, der das Ereignis erläutert ("Audit-Datei wurde gestartet [oder beendet]...am...").
- Die oben erläuterten Makros \${DT} und \${TT}.

Es wird empfohlen, die vordefinierten Texte und Makros beim Anpassen dieser Meldungen beizubehalten. (Eine Ausnahme bildet hierbei das Format, das Sie für Datum und Uhrzeit auswählen.) Dadurch behalten Sie sehr wichtige Informationen bei und können die Meldung schnell in der *Hilfe zu Meldungen* in dem Abschnitt zu DTS finden, der mögliche Gründe und (gegebenenfalls erforderliche) Korrekturmaßnahmen für das Ereignis enthält. Wenn Sie diese Token beibehalten, werden durch die Anpassung standort- oder unternehmensspezifische Werte zur Meldung hinzugefügt, jedoch keine Werte entfernt.

Hinweis: Weitere Informationen finden Sie im Abschnitt "Konfigurationsrichtlinie" in der *DSM-Explorer-Hilfe*.

Makros

In Data Transport Service ist ein Makro ein Zeichensatz, der eine oder mehrere Variablen oder Aktionen darstellt. Sie können einige Makros im Audit-Wert für alle Data Transport-Server oder -Agenten verwenden, während andere nur für die Server, einen bestimmten Server (z. B. den Transfer Object Server) oder einen Agenten gelten. *Erweiterungsmakros* stellen eine besondere Klasse von Makros dar, die Sie selbst definieren können. (Sie können nur Makros anpassen, die im DSM-Explorer zur Verfügung stehen.)

Die Verwendung von Makros stellt für Data Transport Service und CA-Lösungen, die damit zusammenarbeiten, eine erhebliche Erweiterung dar (z. B. Advantage Data Transport). Sie können Makros für jedes Feld angeben, das als Argument verarbeitet oder Teil einer Übertragung werden kann.

Normalerweise werden Makros hauptsächlich aus zwei Gründen verwendet:

- Zum Anpassen der Meldungen, die in der Konsole angezeigt und in die Audit-Protokolldateien geschrieben werden, wenn bestimmte Ereignisse auftreten, an denen ein Data Transport Service-Server oder ein Data Transport-Agent beteiligt sind.
- Zum systematischen Ändern der Namen von Eingabedateien (wenn sie gesendet werden) und Ausgabedateien (wenn Sie empfangen werden) in Datenübertragungen.

Hinweis: Detaillierte Informationen finden Sie im *Referenzhandbuch für DTSLI-Befehle*.

Anpassen von Makros

Wenn Sie die Audit-Werte für Meldungen anpassen, können Sie freien Text und Makros angeben. Während einige Makros für alle DTS-Komponenten gelten, sind andere nur für die Server, einen bestimmten Server (z. B. den TOS) oder den DTS-Agenten relevant.

So passen Sie ein Makro, beispielsweise die Monats- und Tageswerte für den globalen Makro-Modifikator, an:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Standardcomputerrichtlinie", "DSM", "Data Transport Service (DTS)".
2. Klicken Sie auf den Unterknoten der Richtliniengruppe "Makro".

Alle Richtlinien zur Anpassung von Erweiterungsmakros werden im Makro-Fenster angezeigt.

3. Doppelklicken Sie auf das entsprechende Makro.

Das Dialogfeld "Eigenschaften von Einstellung" wird angezeigt.

4. Bearbeiten Sie den Standardwert für das Erweiterungsmakro.
5. Klicken Sie auf "OK".

Das ausgewählte Makro wird angepasst.

Hinweis: Weitere Informationen finden Sie im Abschnitt "Konfigurationsrichtlinie" in der *DSM-Explorer-Hilfe*.

Kapitel 6: Optimieren einer Datenübertragung

Sie müssen eine Übertragungsgruppe für DTS aktivieren, um Daten zu übertragen. Wenn Sie eine Übertragungsgruppe aktivieren, ermittelt die DTS-Optimierungs-Engine die beste Methode für die Datenübertragung. Der Optimierungsprozess umfasst vier Phasen:

Dieses Kapitel enthält folgende Themen:

[Phase 1: Netzwerkruutenanalyse](#) (siehe Seite 69)

[Phase 2: Übertragungseigenschaftenauflösung](#) (siehe Seite 70)

[Phase 3: Auflösen doppelter Übertragungen](#) (siehe Seite 73)

[Phase 4: Auswahl des Übertragungsverfahrens](#) (siehe Seite 73)

Phase 1: Netzwerkruutenanalyse

Phase 1 der Übertragungsoptimierung umfasst die Analyse der DTS-Netzwerktopologie, um zu bestimmen, ob die Daten direkt zwischen zwei Computern oder über mindestens einen anderen (Multi-Hop) übertragen werden müssen. DTS bestimmt anhand der folgenden Regeln, wie Übertragungsrouten innerhalb des Netzwerks erstellt werden sollen:

- Besteht eine Verknüpfung zwischen Quell- und Zielcomputerobjekten?
- Ist das Quellcomputerobjekt Mitglied eines Computercontainerobjekts, und wurde eine Verknüpfung vom Quellcomputercontainerobjekt zum Zielcomputerobjekt definiert?
- Ist das Zielcomputerobjekt Mitglied eines Computercontainerobjekts, und wurde eine Verknüpfung vom Quellcomputerobjekt zum Zielcomputercontainerobjekt definiert?
- Ist das Quellcomputerobjekt Mitglied eines Computercontainerobjekts und das Zielcomputerobjekt Mitglied eines Computercontainerobjekts, und wurde eine Verknüpfung vom Quellcomputercontainerobjekt zum Zielcomputercontainerobjekt definiert?
- Wenn keine direkte Verknüpfung zwischen den beiden Computern oder Computercontainerobjekten, zu denen sie gehören, besteht, untersucht DTS dazwischen liegende Verknüpfungen und Computerobjekte, um festzustellen, ob eine Multi-Hop-Route innerhalb des Netzwerks zwischen den beiden Computern definiert wurde. Wenn eine Multi-Hop-Route definiert wurde, wird diese verwendet. Wenn mehrere Multi-Hop-Routen definiert wurden, wird die Route mit dem kleinsten metrischen Wert verwendet. Wenn zwei oder mehr optimale Routen gefunden werden, wird die erste verwendet.

- Wenn keine Route definiert wurde und weder das Quell- noch das Zielcomputerobjekt zu einer definierten Topologie gehören, wird die Route in eine direkte Verbindung vom Quellcomputerobjekt zum Zielcomputerobjekt aufgelöst.

Weitere Informationen:

[Network Object Server](#) (siehe Seite 26)

Phase 2: Übertragungseigenschaftenauflösung

Die Phase 2 des Übertragungsoptimierungsprozesses umfasst die Auflösung der Übertragungseigenschaften. Diese Übertragungseigenschaften legen die zu verwendenden Datenübertragungseinstellungen fest. Datentransporteigenschaften sind mit allen Netzwerkobjekten verknüpft, einschließlich der Verknüpfungsobjekte, Computercontainerobjekte, Schnittstellenobjekte und Computerobjekte. Um die Priorität der Eigenschaften für Datenübertragungen zu ermitteln, untersucht DTS diese Eigenschaften in folgender Reihenfolge:

1. Verknüpfungsobjekteigenschaften
2. Eigenschaften von Computercontainerobjekten
3. Schnittstellenobjekteigenschaften
4. Computerobjekteigenschaften
5. Standardeigenschaften für die Netzwerkkommunikation

Bei einer nicht definierten (leeren) Eigenschaft für ein Objekt überprüft DTS das nächste Objekt. Wenn also z. B. die Eigenschaft "max_parce_size" für eine Verknüpfung leer ist, prüft DTS die Eigenschaft "max_parcel_size" für das Container-Objekt.

Bei einigen Eigenschaften handelt es sich um GET-Eigenschaften (schreibgeschützt), bei anderen um SET/GET-Eigenschaften (konfigurierbar).

Weitere Informationen:

[Network Object Server](#) (siehe Seite 26)

Verknüpfungsobjekteigenschaften

Wenn eine Verknüpfung zwischen Computerobjekten, Computercontainerobjekten oder beidem besteht, werden die Eigenschaftswerte dieser Verknüpfung verwendet. Wenn zum Beispiel eine Übertragung zwischen Computer A und D gestartet wird, werden die Eigenschaften der Verknüpfung zwischen Computer A und B geprüft, um zu bestimmen, wie die erste Hälfte der Multi-Hop-Übertragung ablaufen soll, und die Eigenschaften der Verknüpfung zwischen Computer B und D für die zweite Hälfte der Übertragung.

Wenn die Übertragung keine Verknüpfung zwischen den Computer- und den Computercontainerobjekten enthält, werden als Nächstes die Eigenschaften des Computercontainerobjekts geprüft.

Eigenschaften von Computercontainerobjekten

Mit Hilfe von Computercontainerobjekten können Administratoren Netzwerkeigenschaften für eine Gruppe von Computerobjekten festlegen. Wenn zum Beispiel eine Übertragung zwischen Computerobjekten gestartet wird, die durch keine Verknüpfung verbunden sind, und die Eigenschaften dieser Computerobjekte über ein Computercontainerobjekt festgelegt werden, werden die Eigenschaften dieses Computercontainerobjekts geprüft, um festzustellen, wie die Übertragung ablaufen soll.

Wenn weder eine Verknüpfung noch ein Computercontainerobjekt vorhanden ist, werden als Nächstes die Schnittstellenobjekte und deren Eigenschaften geprüft.

Schnittstellenobjekteigenschaften

Schnittstellenobjekte definieren in der Regel eine physische Schnittstelle, die mit einem bestimmten Computer verknüpft ist. Der Schnittstelle sind bestimmte Protokollmerkmale zugeordnet. Durch die Zuweisung einer Prioritätseigenschaft zur Schnittstelle können Sie die Reihenfolge der Auswertung der Schnittstelle festlegen, wenn Sie das für eine Übertragung zu verwendende Punkt-zu-Punkt-Protokoll angeben. Schnittstellen, die mit dem Responder-Computer verknüpft sind, werden mit denen des als Initiator agierenden Computers verglichen, bis eine Schnittstelle mit übereinstimmendem Punkt-zu-Punkt-Protokoll gefunden wird.

Computer können mit mehreren Schnittstellen verknüpft sein. Die geeignete Schnittstelle wird nach aufsteigender Priorität abhängig von einer Übereinstimmung für den Punkt-zu-Punkt-Protokollparameter für den Initiator- und Responder-Computer ermittelt.

Ein Prioritätswert von 1 (der höchsten Priorität) deutet beispielsweise darauf hin, dass die Schnittstelle zuerst überprüft wird. Der Wert 0 (die Standardeinstellung) deutet auf eine nicht zugewiesene Priorität hin. In diesem Fall wird die Schnittstelle zuletzt überprüft.

Bei der Überprüfung von Schnittstellen werden die Schnittstellen, die mit dem Responder-Computer verknüpft sind, mit denen des als Initiator agierenden Computers verglichen, bis eine Schnittstelle mit übereinstimmendem Punkt-zu-Punkt-Protokoll gefunden wird. Der Responder-Computer bestimmt daher das Protokoll, unabhängig davon, ob der antwortende Computer Daten empfängt oder sendet. (Der Responder-Computer sendet die Daten, wenn der als Initiator agierende Computer sie abrufen.)

Es gibt auch den Fall, bei dem ein Rechner Daten von einem anderen Computer abrufen. In diesem Szenario ist der abrufende (und empfangende) Computer der Initiator, während der die Daten sendende Computer der Responder ist. Unabhängig von der Datenrichtung werden die mit dem Responder-Rechner verknüpften Schnittstellen gegen die des Initiator-Computers geprüft, bis ein übereinstimmendes Punkt-zu-Punkt-Protokoll gefunden wird.

Kommunikationseinstellungen

Wenn keine geeignete Schnittstelle gefunden werden kann, werden die Kommunikationseinstellungen der einzelnen Computerobjekte verwendet, um zu ermitteln, wie die Übertragung erfolgen soll. Wenn eine Übertragung gestartet wird, bestimmen die Eigenschaften des Initiator-Computerobjekts den zu verwendenden Drosselungsfaktor, während die Eigenschaften des Responder-Computerobjekts das Protokoll festlegen. Die Paketgröße hängt von der Größe des kleineren Paketes der beiden Computer in der Übertragung ab.

Je nach den Einstellungen der Netzwerkeigenschaften des Computerobjekts und der Konfiguration der Verknüpfungen können Sie Zwischencomputer während der Übertragung verwenden. Der Initiator- und Responder-Computer sowie die Netzwerkeigenschaften, auf die anschließend verwiesen wird, ändern sich im Laufe der Übertragung.

Phase 3: Auflösen doppelter Übertragungen

Die Phase 3 des Übertragungsoptimierungsprozesses besteht im Auflösen doppelter Übertragungen. Bei diesem einfachen Prozess wird geprüft, ob Übertragungen in der aktivierten Übertragungsgruppe identisch sind. Wenn identische Übertragungen gefunden werden, werden sie zu einer einzigen Übertragung zusammengefasst. Dies trifft zu, wenn mehrere Übertragungen in Multi-Hops erweitert wurden, die alle über einen einzelnen Zwischencomputer laufen. In der Regel wird die erste Hop-Hälfte in eine einzelne Übertragung aufgelöst. Zwei Übertragungen gelten als identisch, wenn Folgendes übereinstimmt:

- Eingabedaten
- Initiator-Computer
- Ausgabedaten
- Responder-Computer
- Initiator- und Responder-Sicherheits-Token (Benutzer und Kennwort)
- Alle Filter
- Positionen in einer Hop-Sequenz

Hinweis: Eine Punkt-zu-Punkt-Übertragung am Ende einer Hop-Sequenz kann niemals als Duplikat einer Übertragung in der Mitte einer Hop-Sequenz betrachtet werden.

Weitere Informationen:

[Transfer Object Server \(TOS\)](#) (siehe Seite 29)

Phase 4: Auswahl des Übertragungsverfahrens

Die letzte Phase des Übertragungsoptimierungsprozesses, die Phase 4, umfasst die Auswahl eines geeigneten Übertragungsverfahrens.

DTS unterstützt drei Datenübertragungsverfahren.

- Punkt-zu-Punkt
- Fanout
- Punkt-zu-Viele

Standard ist das Punkt-zu-Punkt-Verfahren. DTS entscheidet anhand der Angabe der aktivierten Übertragungen und der Netzwerkkonfiguration automatisch, welches Verfahren verwendet wird.

Wenn Mehrfachübertragungen über eine Übertragungsgruppe aktiviert werden, umfasst das Punkt-zu-Punkt-Verfahren viele Lesevorgänge, viele Sendevorgänge (über das Netzwerk) und viele Schreibvorgänge für jedes Paket der verarbeiteten Daten. Fanout umfasst jedoch einen einzelnen Lesevorgang, viele Sendevorgänge und viele Schreibvorgänge.

Das effizienteste Verfahren ist Punkt-zu-Viele, also ein Lesevorgang, ein Sendevorgang und mehrere Schreibvorgänge. Fanout oder Punkt-zu-Viele kann jedoch nur ausgeführt werden, wenn die Übertragungsobjekte bestimmte gemeinsame Eigenschaftswerte aufweisen.

Weitere Informationen:

[Transfer Object Server \(TOS\)](#) (siehe Seite 29)

Übertragungsressourcennutzung

Beachten Sie bei der Auswahl der Übertragungsverfahren folgende Überlegungen:

- Broadcast ist weniger ressourcenintensiv als Fanout.
- Fanout ist weniger ressourcenintensiv als Punkt-zu-Punkt.

Wenn die Parameter für Broadcast bei einer Eins-zu-Viele-Übertragung angegeben werden (und wenn die Übertragung nicht in eine auf dem TOS vorhandene Übertragung von der doppelten Übertragungsauflösung aufgelöst wird), wird die Auswahl von Broadcast gegenüber Fanout und die Auswahl von Fanout gegenüber Punkt-zu-Punkt bevorzugt. Die bevorzugte Protokollreihenfolge ist unabhängig von den Vorrangregeln für die Auswahl von Parameterwerten.

Beziehung zwischen Broadcasts und Verknüpfungs- oder Containereigenschaften

Wenn Sie Broadcast-Parameter für einen Container, aber keine Verknüpfung zu diesem Container festlegen, wird das Broadcast-Protokoll trotzdem verwendet.

Punkt-zu-Punkt-Übertragungen

Bei Punkt-zu-Punkt-Übertragungen werden Daten von einem einzelnen Initiatorcomputer zu einem einzelnen Respondercomputer gesendet. Das ist der einfachste Übertragungstyp, da Daten nur einmal zu einem einzigen Ziel gesendet werden. Punkt-zu-Punkt-Übertragungen enthalten die folgenden Eigenschaften:

Punkt-zu-Punkt-Protokoll

Legt das Kommunikationsprotokoll für die Punkt-zu-Punkt-Übertragung fest.

Punkt-zu-Punkt-Adresse

Gibt die für Punkt-zu-Punkt-Übertragungen an diesen Computer zu verwendende Adresse an.

Punkt-zu-Punkt-Parameter

Gibt Parameter für das Punkt-zu-Punkt-Protokoll an, die bei Punkt-zu-Punkt-Übertragungen an diesen Computer zu berücksichtigen sind.

Hinweis: Detaillierte Informationen finden Sie im *Referenzhandbuch für DTSCLI-Befehle*.

Fanout-Übertragungen

Bei Fanout-Übertragungen werden Daten zu mehreren Responder-Computern unter Verwendung eines direkten Punkt-zu-Punkt-Kommunikationsprotokolls gesendet. Das Fanout-Übertragungsverfahren kann in jedem Netzwerk eingesetzt werden. Punkt-zu-Punkt-Kommunikationsverknüpfungen werden mit allen Endsystemen aufgebaut. Die Quelldaten werden dann einmal gelesen und viele Male über jede Verbindung gesendet. Dies kann die Effizienz beträchtlich erhöhen, wenn die Lese-Eingabe/Ausgabe langsam ist oder eine langsame/CPU-Lesefilterung festgelegt ist (zum Beispiel Komprimierung oder Verschlüsselung).

Hinweis: Das Fanout-Übertragungsverfahren kann nur verwendet werden, wenn Eingabe und Initiator-Computer für alle Übertragungsobjekte in der Übertragungsgruppe identisch sind.

Fanout-Übertragungen enthalten die folgenden Eigenschaften:

Fanout-Protokoll

Legt das Kommunikationsprotokoll für die Fanout-Übertragung fest.

Fanout-Adresse

Gibt die zu verwendende Adresse an, wenn an diesen Computer eine Fanout-Datenübertragung gesendet wird.

Fanout-Parameter

Legt spezielle Parameter fest, die dem Protokoll hinzugefügt werden müssen. Fanout ist ein Übertragungsverfahren, bei dem Daten gesendet werden, indem sie einmal gelesen und dann mehrfach zu den jeweiligen Zielrespondern gesendet werden.

Hinweis: Detaillierte Informationen finden Sie im *Referenzhandbuch für DTSCLI-Befehle*.

Fanout-Übertragungskriterien

Mehrere Punkt-zu-Punkt-Übertragungen, die zur gleichen Zeit (also in der gleichen Übertragungsgruppe) aktiviert werden, können zu einer Fanout-Übertragung kombiniert werden, wenn Folgendes gleich ist:

- Eingabedaten
- Ausgabedaten
- Initiator-Computer
- Sicherheits-Token des Initiators (Initiator-Benutzer und -Kennwort) für jede Übertragung
- Sicherheits-Token des Responders (Responder-Benutzer und -Kennwort) für jede Übertragung
- Read Parcel- und Read File-Filter
- Paketgröße

Punkt-zu-Viele-Übertragungen

Bei Punkt-zu-Viele-Übertragungen werden Daten über ein Punkt-zu-Viele-Protokoll wie beispielsweise BCAST (IP-Broadcast) oder MCAST (IP-Multicast) an mehrere Responder-Computer gesendet. Sie können das Punkt-zu-Viele-Übertragungsverfahren nur in IP-basierten Netzwerken verwenden, da hierbei die Funktionen der BCAST- und MCAST-Protokolle (die wiederum UDP verwenden) eingesetzt werden.

Wichtig! DTS unterstützt die IPv4-Broadcast- und die IPv4/IPv6-Multicast-Adressierung. Das Eins-zu-Viele-Übertragungsverfahren kann nur mit IPv4-Adressen verwendet werden. Falls Sie über ein IPv6-Netzwerk eine Übertragung im Broadcast-Verfahren durchführen möchten, verwenden Sie das MCAST-Protokoll mit den entsprechenden IPv6-Multicast-Adressen.

Hinweis: Das Eins-zu-Viele-Übertragungsverfahren kann nur verwendet werden, wenn Eingabe, Initiator-Computer und Ausgabe für alle Übertragungsobjekte in der Übertragungsgruppe identisch sind.

Punkt-zu-Viele-Übertragungen enthalten die folgenden Eigenschaften:

Punkt-zu-Viele-Protokoll

Legt das Kommunikationsprotokoll für die Punkt-zu-Viele-Übertragung fest.

Punkt-zu-Viele-Netzwerkadresse

Bestimmt die primäre Netzwerkadresse für eine Datenübertragung über ein Punkt-zu-Viele-Protokoll, zum Beispiel Broadcast oder Multicast, an diesen Computer.

Punkt-zu-Viele-Parameter

Gibt spezielle Parameter an, die an das Protokoll übergeben werden. Punkt-zu-Viele ist ein Übertragungsverfahren, bei dem Daten einmal gelesen und einmal an alle Ziel-Responder gleichzeitig gesendet werden.

Hinweis: Detaillierte Informationen finden Sie im *Referenzhandbuch für DTSCLI-Befehle*.

Punkt-zu-Viele-Übertragungskriterien

Mehrere Punkt-zu-Punkt-Übertragungen, die zur gleichen Zeit (also in der gleichen Übertragungsgruppe) aktiviert werden, können zu einer Punkt-zu-Viele-Übertragung kombiniert werden, wenn Folgendes gleich ist:

- Eingabedaten
- Ausgabedaten
- Initiator-Computer
- Sicherheits-Token des Initiators (Initiator-Benutzer und -Kennwort) für jede Übertragung
- Sicherheits-Token des Responders (Responder-Benutzer und -Kennwort) für jede Übertragung
- Alle Filter
- Punkt-zu-Viele-Protokolleigenschaften (BCAST oder MCAST)
- Punkt-zu-Viele-Netzwerkadresseneigenschaften (dürfen nicht leer sein)

Kapitel 7: Übertragungsprotokolle und -verfahren

Dieses Kapitel enthält eine Übersicht über die Datenübertragungsprotokolle und -verfahren von Data Transport Service.

Dieses Kapitel enthält folgende Themen:

[Protocol Wrapper Interface \(PWI\)](#) (siehe Seite 79)

[TCP](#) (siehe Seite 79)

[UDP](#) (siehe Seite 79)

[IP-Broadcast oder BCAST](#) (siehe Seite 80)

[IP-Multicast oder MCAST](#) (siehe Seite 81)

Protocol Wrapper Interface (PWI)

DTS unterstützt eine Reihe verschiedener Kommunikationsprotokolle und Datenübertragungsverfahren. Über PWI (Protocol Wrapper Interface) ist DTS von anderen Kommunikationsprotokollen isoliert. PWI ruft weitere Protokoll-Wrapper-Funktionen auf, die die entsprechenden protokollspezifischen Funktionen aufrufen. Der in DTS verwendete Protokoll-Wrapper-Code gewährleistet die Zuverlässigkeit.

Hinweis: Detaillierte Informationen finden Sie im *Referenzhandbuch für DTSCLI-Befehle*.

TCP

Das TCP-Protokoll ist robust, zuverlässig und effizient. Bei langsamen, unzuverlässigen Netzwerken oder störanfälligen Kommunikationswegen ist TCP die beste Wahl. DTS verwendet das Standardprotokoll TCP.

UDP

Das UDP-Protokoll ist schnell, jedoch unzuverlässig. Datenpakete können verloren gehen, und UDP meldet dies in den meisten Fällen nicht. UDP ist eine gute Wahl, wenn Sie über ein gutes, sauberes, zuverlässiges und leistungsstarkes Netzwerk verfügen. Der Protokoll-Wrapper von DTS stellt durch Rücksenden verlorener Datenpakete sicher, dass Ihre Daten zuverlässig übertragen werden. Wenn UDP in einem ausgelasteten Netzwerk verwendet wird, können mehr Probleme verursacht als gelöst werden, da Datenpakete fortlaufend erneut gesendet werden.

IP-Broadcast oder BCAST

BCAST oder IP-Broadcast ist ein Protokoll, mit dem ein Initiator ein einzelnes Datenpaket an mehrere Endsysteme gleichzeitig senden kann. Das Datenpaket wird an alle angeschlossenen Computer in einem bestimmten IP-Subnetz gesendet.

Sie können keine Daten über Subnetze oder WAN senden. DTS verwendet Broadcast, wenn Sie die gleichen Quelldaten von einem einzelnen Computer an den gleichen Zielspeicherort in diesen Endsystemen im selben lokalen Subnetz senden. Broadcast ist ein effizientes Verfahren zur Übertragung von Daten, insbesondere, wenn die Anzahl der Endsysteme sehr hoch ist.

Wichtig! DTS unterstützt die IPv4-Broadcast- und die IPv4/IPv6-Multicast-Adressierung. Das Eins-zu-Viele-Übertragungsverfahren kann nur mit IPv4-Adressen verwendet werden. Falls Sie über ein IPv6-Netzwerk eine Übertragung im Broadcast-Verfahren durchführen möchten, verwenden Sie das MCAST-Protokoll mit den entsprechenden IPv6-Multicast-Adressen.

Berechnen einer Broadcast-Adresse

Sie können die Broadcast-Adresse eines Computers anhand des folgenden logischen Algorithmus berechnen:

Broadcast-Adresse = (Subnetzmaske AND IP-Adresse)
OR (NOT(Subnetzmaske))

So berechnen Sie eine Broadcast-Adresse:

1. Übersetzen Sie die Subnetzmaske und die IP-Adresse des Verteilungssystems in die jeweiligen binären Entsprechungen.

Die IP-Adresse 172.16.29.156 und die Subnetzmaske 255.255.0.0 würden beispielsweise folgendermaßen ausgedrückt:

IP-Adresse = 10101100.00010000.00011101.10011100

Subnetzmaske = 11111111.11111111.00000000.00000000

Mit AND lautet das verkettete Ergebnis wie folgt:

10101100.00010000.00000000.00000000

2. Führen Sie eine binäre OR-Operation mit der Umkehrung der Subnetzmaske durch. Hierdurch erhalten Sie die Broadcast-Adresse für das Netzwerk, zu dem der Broadcast-Computer gehört, sowie die entsprechende Subnetzmaske.

Mit der IP-Adresse und der Subnetzmaske von Schritt 1 wird dies folgendermaßen ausgedrückt:

Subnetzmaske AND IP-Adresse =

10101100.00010000.00000000.00000000 (171.16.0.0)

NOT (Subnetzmaske)=

00000000.00000000.11111111.11111111 (0.0.255.255)

Mit OR ergibt sich die folgende Broadcast-Adresse:

172.16.11111111.11111111 = (172.16.255.255)

IP-Multicast oder MCAST

IP-Multicast ist eine relativ neue Netzwerktechnologie mit ähnlichen Funktionen wie Broadcast, außer dass die Endsysteme sich an einer beliebigen Stelle im Netzwerk befinden können. Bevor Daten übertragen werden, werden die Endsysteme zu einer Multicast-Gruppe verbunden. Daten, die an die Multicast-Adresse der Gruppe gesendet werden, werden von allen Mitgliedern der Multicast-Gruppe empfangen. Eine Multicast-Adresse identifiziert eine Multicast-Gruppe. Gültige Multicast-Adressen, die Sie für DTS verwenden können, liegen im Bereich von 224.0.1.0 bis 238.255.255.255 (Adressen mit globalem Wirkungsbereich).

Hinweis: Die Legacy-Hardware (zum Beispiel Router) unterstützt Multicast möglicherweise nicht.

DTS verwendet dynamische Multicast-Gruppen, die nach Abschluss der Übertragung entfernt und nicht mehr benötigt werden. Bestimmte Unternehmen oder Produkte sind möglicherweise bereits offiziell für die Verwendung von Multicast-Adressen am unteren Ende des Bereichs registriert. Daher ist es am besten, Multicast-Adressen im oberen Bereich zu wählen.

Wichtig! DTS unterstützt die IPv4-Broadcast- und die IPv4/IPv6-Multicast-Adressierung. Das Eins-zu-Viele-Übertragungsverfahren kann nur mit IPv4-Adressen verwendet werden. Falls Sie über ein IPv6-Netzwerk eine Übertragung im Broadcast-Verfahren durchführen möchten, verwenden Sie das MCAST-Protokoll mit den entsprechenden IPv6-Multicast-Adressen.

Reservierte und registrierte Multicast-Adressen

Die Internet Assigned Numbers Authority (IANA) verwaltet eine Liste von registrierten IP-Multicast-Gruppen, die in der folgenden Tabelle aufgelistet sind:

Adresse	Reserviert für
224.0.0.0	Die Basisadresse; kann keiner Gruppe zugewiesen werden.
224.0.0.1 bis 224.0.0.255	Adressen im lokalen Bereich; werden für Routing-Protokolle und andere Topologie-Erkennungs- oder Wartungsprotokolle auf niedriger Ebene verwendet. Multicasts in diesem Bereich werden unabhängig von TTL nie außerhalb des lokalen Netzwerks weitergeleitet. Multicast-Router dürfen kein Multicast-Datagramm mit einer Zieladresse in diesem Bereich weiterleiten, unabhängig von deren TTL.
224.0.1.0 bis 238.255.255.255	Adressen mit globalem Wirkungsbereich; wird für Multicast-Gruppenadressen verwendet. Zu den bekanntesten Gruppen gehören: Alle Systeme in diesem Subnetz (224.0.0.1) Alle Router in diesem Subnetz (224.0.0.2) Alle DVMRP-Router (224.0.0.4) Alle OSPF-Router (224.0.0.5) IETF-1-Audio (224.0.1.11) IETF-1- Video (224.0.1.12) AUDIONEWS (224.0.1.7) MUSIC-SERVICE (224.0.1.16)
239.0.0.0 bis 239.255.255.255	Adressen im administrativen Bereich, werden für <i>private Domänen</i> bzw. lokale Anwendungen an einem Standort und <i>nicht</i> für Internet-Anwendungen verwendet.

UDP-Betrieb und Einschränkungen

Multicast bietet keine garantierte Lieferung; es sendet seine Pakete mit Hilfe von UDP, was unzuverlässiger ist als TCP. UDP ist ein einfaches, unzuverlässiges Datagrammprotokoll, das die SOCK_DGRAM-Abstraktion für die Internetprotokollfamilie unterstützt. Es befindet sich auf einer Ebene direkt über dem Protokoll (IP). UDP-Sockets sind verbindungslos und werden in der Regel mit den Systemaufrufen "sendto", "sendmsg", "recvfrom" und "recvmsg" verwendet. Die Verwendung von Multicast und UDP unterliegt folgenden Nachteilen und Einschränkungen:

- UDP-Pakete können auf unterschiedliche Weise verloren gehen oder verworfen werden, zum Beispiel wenn ein Fehler des zugrunde liegenden Kommunikationsmechanismus vorliegt.
- UDP implementiert eine Prüfsumme über den Datenanteil des Pakets. Wenn die Prüfsumme eines empfangenen Pakets fehlerhaft ist, wird das Paket ohne entsprechende Benachrichtigung des Absenders verworfen.
- UDP-Sockets speichern eine beschränkte Warteschlange eingegangener Pakete. Datagramme, die darüber hinaus eingehen, werden ohne entsprechende Benachrichtigung verworfen.
- UDP empfängt und verarbeitet ICMP-Fehlermeldungen (Internet Control Message Protocol) als Reaktion auf UDP-Pakete. Hierbei gelten folgende Einschränkungen:
 - ICMP-Meldungen wegen einer Löschung der Quelle werden ignoriert.
 - Bei ICMP-Meldungen wegen nicht erreichbarem Ziel, abgelaufener Zeit oder Parameterprobleme wird der Socket von seinem Peer getrennt. Spätere Versuche, Pakete mit demselben Socket zu senden, geben einen Fehler zurück.
- UDP kann nicht garantieren, dass Pakete in der Reihenfolge geliefert werden, in der sie gesendet wurden.
- UDP erstellt möglicherweise während des Kommunikationsvorgangs doppelte Pakete.
- Die Anwendung, die UDP verwendet, muss die Lieferung eines UDP-Pakets überprüfen. Garantierte Lieferung ist eine Schlüsselfunktion von DTS. Die DTS-Agenten auf dem Initiator und Responder sorgen gemeinsam für eine ordnungsgemäße Lieferung von Daten, zu denen auch UDP-Pakete gehören können.
- UDP-Pakete erhalten in einem umgeleiteten Netzwerk niedrige Priorität. Wenn ein Netzwerk ausgelastet ist und Pakete gelöscht werden, werden die UDP-Pakete zuerst gelöscht. Wenn der Router in einer DTS-Umgebung ein Paket löscht, benachrichtigt der antwortende Agent den Initiator, dass Daten gelöscht wurden, und fordert ein erneutes Senden an. Der Initiator sendet das Paket anschließend erneut. Da ständig Daten erneut gesendet werden müssen, erhöht sich der Netzwerkverkehr, was zu mehr verlorenen Paketen führt.

- Wenn ein Router mehrmals Multicast-Pakete an alle Subnetze sendet, erhöht sich der Netzwerkverkehr drastisch. Multicast-Meldungen werden an alle Subnetze gesendet. Da die Router nicht wissen können, welche Subnetze über Responder für diese Daten verfügen, werden die Daten an alle Subnetze gesendet.

Empfehlungen für Multicast-Gruppen

Um für eine garantierte Lieferung zu sorgen, empfehlen wir, Multicast- und Broadcast-Gruppen mit höchstens 50 Computern pro Gruppe einzurichten. Ein zuverlässiges Netzwerk kann die Anforderung einer Multicast- oder Broadcast-Übertragung erfüllen, wenn die Anzahl der Computer pro Gruppe unter 50 liegt. Wenn diese Gruppen aus mehr als 50 Computern bestehen, löscht das Netzwerk mehr UDP-Pakete, und es kommt somit zu mehr Wiederholungen. In dem Maße, in dem die Anzahl der Wiederholungen steigt, sinkt die Effizienz des Netzwerks.

Netzwerkconfiguration für Multicast

Standardmäßig ist Multicast in Netzwerken deaktiviert. Der Netzwerkadministrator muss sicherstellen, dass Multicast im gesamten Netzwerk aktiviert ist. Er muss insbesondere Multicast auf allen Routern und Schaltern zwischen dem initiierenden und dem antwortenden DTS-Agentencomputer aktivieren, die Teil einer Multicast-Übertragung sind.

Hinweis: Nicht alle Router und Schalter unterstützen Multicast. Die Schalter müssen sich mindestens auf der zweiten Ebene befinden, damit Multicast unterstützt wird.

Plattformeinschränkungen für Multicast

Einige Plattformen unterstützen Multicast nicht. Multicast-Unterstützung ist die Funktion des Protokollstapels und der Netzwerkschnittstelle an jeder Plattform. Auf einigen Protokollstapeln oder Netzwerkkarten müssen Sie Multicast aktivieren und/oder konfigurieren. Genauere Informationen und Voraussetzungen finden Sie in der Dokumentation zur jeweiligen Plattform.

Multicast-Internetlinks

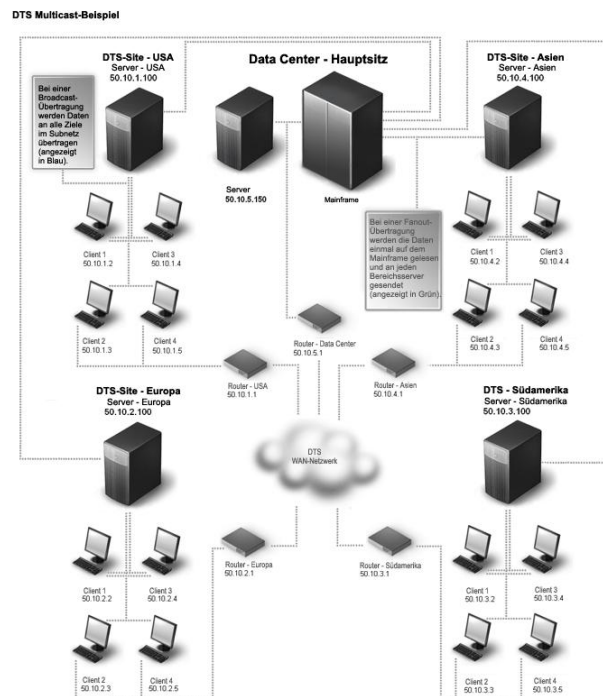
Weitere Einzelheiten zur Konfiguration und zum Test eines Netzwerks für Multicast finden Sie in den Multicast-Informationen in den folgenden Internetquellen. Sie können auch im Internet nach weiteren Artikeln suchen.

- Die Multicast-Anleitungen auf der Website des Linux Documentation Project <http://www.tldp.org>. Dabei handelt es sich um eine Linux-Seite, aber eine Vielzahl der Multicast-Informationen gilt für alle Plattformen, die Multicast verwenden.
- Die Website der Multicast Working Group <http://multicast.internet2.edu>.
- Die Multicast-Startseite der University of Southern California <http://netweb.usc.edu/multicast>.

Verwenden mehrerer Liefermethoden

DTS unterstützt verschiedene Liefermethoden und -protokolle. Prüfen Sie alle, um zu bestimmen, welche Kombination für Ihre Umgebung die beste ist. In den meisten DTS-Netzwerken ist es sinnvoller, nicht nur Multicast allein zu verwenden.

Die meisten Netzwerkkonfigurationen enthalten eine Kombination aus Punkt-zu-Punkt-, Fanout-, Broadcast- und Multicast-Übertragungen. Das folgende Beispiel zeigt eine DTS-Konfiguration, in der die Verknüpfungen zu und vom Netzwerk (Wolke) langsame Satellitenverbindungen mit 56Kb darstellen.



Das Netzwerk sollte mit möglichst wenig Verkehr belastet werden, solange Daten an alle Desktop-Rechner auf der ganzen Welt übertragen werden. Um dieses Ziel zu erreichen, können Sie mit der WorldView 2D-Karte die Computer und Verknüpfungen in unserem Netzwerk konfigurieren. Ziel ist es, die effizienteste Liefermethode für jeden Übertragungstyp (global oder lokal) in diesem Szenario zu verwenden.

Hinweis: Weitere Informationen oder Anweisungen zur Verwendung der 2D-Karte finden Sie in der WorldView-Dokumentation oder in der Online-Hilfe.

Konfigurieren der Server für die Verwendung von Fanout für kontinentübergreifende Übertragungen

Sie können Server für die Verwendung einer Fanout-Übertragung konfigurieren. In unserem Multicast-Beispiel können Sie ein Fanout vom z/OS-Mainframe im Rechenzentrum zum Server auf jedem Kontinent durchführen, da die Satellitenverbindung unzuverlässig ist. Ein Fanout liest die Daten einmal und schreibt sie einmal auf jeden Server. Dadurch ist das Fehlerrisiko geringer als bei mehreren gleichzeitigen Übertragungen.

So konfigurieren Sie die Server für Fanout:

1. Öffnen Sie DTS Business Process View in Ihrer WorldView 2D-Karte.
2. Navigieren Sie zum Ordner "Netzwerk-Administration und -Überwachung".
3. Erstellen Sie einen DT-Container, und legen Sie alle Server darin ab.
4. Markieren Sie den Container, klicken Sie mit der rechten Maustaste, und wählen Sie im Kontextmenü die Option "DTS-Details öffnen" aus.

Das Dialogfeld "Objektdetails" wird angezeigt.

5. Wählen Sie im Feld "Fanout-Protokoll" die Option "TCP" aus der Dropdown-Liste aus. Vergewissern Sie sich, dass alle anderen Felder leer sind, und klicken Sie auf "OK".

DTS ist so konfiguriert, dass Fanout jedes Mal verwendet wird, wenn Übertragungen mit einem Computer im Container gesendet oder empfangen werden müssen.

Verwenden von Broadcast für lokale Übertragungen

Broadcast ist die beste Option für Server-zu-Desktop-Übertragungen, da diese Übertragungen ein lokales Netzwerk ohne Router verwenden. Wenn Sie DTS konfigurieren, geben Sie Broadcast für Übertragungen an, bei denen Daten vom Server an alle Desktops gesendet werden.

Erstellen von Containern und Verknüpfungen für Desktops

Sie können Container und Verknüpfungen für Ihr DTS-Netzwerk erstellen.

So erstellen Sie Container und Verknüpfungen für Desktops:

1. Öffnen Sie DTS Business Process View in Ihrer WorldView 2D-Karte.
2. Navigieren Sie zum Ordner "Netzwerk-Administration und -Überwachung".
3. Erstellen Sie mehrere DT-Container namens "US-Desktops", "Europa-Desktops", "Asien-Desktops" und "Südamerika-Desktops".
4. Platzieren Sie in jedem Container die Desktops, die zu der jeweiligen Region gehören.
5. Erstellen Sie separate DT-Verknüpfungen auf der 2D-Karte, die jeden Kontinent-Container mit dem Server für diesen Kontinent verbinden.

Erstellen Sie zum Beispiel eine Verknüpfung, die den US-Server mit dem US-Desktop-DT-Container verbindet, und erstellen Sie eine Verknüpfung, die den Europa-Server mit dem Europa-Desktop-DT-Container verbindet.

6. Gehen Sie folgendermaßen vor, um die neu erstellten DT-Verknüpfungen zu konfigurieren:
 - a. Markieren Sie jede einzelne Verknüpfung, klicken Sie mit der rechten Maustaste, und wählen Sie im Kontextmenü die Option "DTS-Details öffnen" aus.
 - b. Das Dialogfeld "Objektdetails" wird angezeigt.
 - c. Wählen Sie im Punkt-zu-Viele-Protokoll in der Dropdown-Liste die Option "Broadcast" aus.
 - d. Geben Sie in das Feld "Netzwerkadresse" die Broadcast-Adresse ein.
 - e. Geben Sie in das Feld "Parameter" die Subnetzmaske der Verknüpfung ein.
 - f. Vergewissern Sie sich, dass alle anderen Felder leer sind.
 - g. Klicken Sie auf "OK", um das Dialogfeld zu schließen.

Hinweis: Wiederholen Sie diese Schritte für jede Verknüpfung. Geben Sie unbedingt "Broadcast" und die richtige Netzwerkadresse sowie den richtigen Wert für Netzwerkmaske ein.

Kapitel 8: Diagnose und Fehlerbehebung

Dieses Kapitel enthält Informationen zu Diagnosetools und Hinweise zur Fehlerbehebung bei Data Transport Service.

Dieses Kapitel enthält folgende Themen:

[Erfassungstool für Protokolldateien dsminfo](#) (siehe Seite 89)

[CAM-Kommunikation funktioniert nicht](#) (siehe Seite 90)

[Multicast-Übertragung fehlgeschlagen \(Windows\)](#) (siehe Seite 90)

[Multicast-Übertragung fehlgeschlagen \(UNIX\)](#) (siehe Seite 91)

[Business Process Views-Installation schlägt fehl](#) (siehe Seite 92)

[DFÜ-Unterstützung funktioniert nicht](#) (siehe Seite 92)

[Technischer Support](#) (siehe Seite 93)

Erfassungstool für Protokolldateien dsminfo

CA Technologies stellt das Tool "dsminfo" zur Verfügung, das Diagnoseinformationen von Systemen erfasst, in denen CA ITCM installiert ist. Die gesammelten Daten werden in eine einzelne Datei komprimiert, die Protokolldateien, Systeminformationen, Verzeichnisstrukturen sowie Registrierungs- und Umgebungsinformationen enthält. Dieses Diagnose-Tool ist befindet sich auf dem CA ITCM Produktinstallationsdatenträger im Ordner "DiagnosticTools".

Wenn Sie ein Problem mit CA ITCM reproduzieren können, führen Sie den folgenden Befehl aus, um die Trace-Ebene in DETAIL zu ändern:

```
cftrace -c set -l DETAIL
```

Reproduzieren Sie das Problem und sammeln Sie die Diagnoseinformationen mit dem Tool "dsminfo".

Hinweise:

Weitere Information zu diesem Tool finden Sie in der Datei DSMInfoReadMe.txt im Ordner "DiagnosticTools" auf dem Datenträger für die Produktinstallation.

Das Tool "dsminfo" erzeugt standardmäßig ".7z"-Dateien. Diese Dateien bieten bessere Verdichtung als ZIP-Dateien, so ist es leichter, sie nach CA Technologies hochzuladen.

CAM-Kommunikation funktioniert nicht

Symptom:

Während der DTS-Dateiübertragung tritt ein Kommunikationsproblem zwischen meinem Responder-Computer und meinem Initiator-Computer auf.

Lösung:

Stellen Sie sicher, dass für CA Message Queuing (CAM) ein offener Pfad im Netzwerk besteht. Geben Sie hierzu folgenden Befehl ein:

```
camping Hostname | IP-Adresse
```

Führen Sie diesen Befehl über den Responder und den Initiator her aus, um sicherzustellen, dass eine Kommunikation in beide Richtungen möglich ist. Wenn ein TOS an der Übertragung beteiligt ist, führen Sie den Befehl "camping" zwischen dem TOS-Computer und dem Initiator (in beiden Richtungen) aus.

CAM wird für die Kommunikation zwischen dem TOS und dem DTS-Agenten verwendet, jedoch nicht für die Kommunikation zwischen DTS-Servern (TOS, NOS und SOS). Verwenden Sie deshalb den Befehl "camping" nur zum Testen der Kommunikation zwischen einem TOS und seinen Agenten.

Multicast-Übertragung fehlgeschlagen (Windows)

Symptom:

Wie kann ich einen Multicast-Übertragungsfehler auf Windows beheben?

Lösung:

Windows enthält das Hilfsprogramm *mrinfo*, das Sie für die Multicast-Fehlerbehebung verwenden können. Anweisungen zur Verwendung von *mrinfo* finden Sie in der Dokumentation und der Windows-Online-Hilfe.

Hinweis zu den Hilfsprogrammen von UNIX und Microsoft: Die meisten Diagnose- und Konfigurationsdienstprogramme sind hardware-spezifisch. Das hier erläuterte Hilfsprogramm von UNIX oder Microsoft ist im Lieferumfang bestimmter Versionen der entsprechenden Betriebssysteme enthalten. Weitere Informationen und Support zu Hilfsprogrammen für Computer, Router, Switches und Netzwerke erhalten Sie in der jeweiligen Online-Hilfe und Dokumentation des Anbieters.

Multicast-Übertragung fehlgeschlagen (UNIX)

Symptom:

Wie kann ich einen Multicast-Übertragungsfehler auf UNIX-Computern beheben?

Lösung:

Das UNIX-Hilfsprogramm *mtrace* vereinfacht die Multicast-Fehlerbehebung. Einzelheiten zu den Funktionen dieses Hilfsprogramms und Anweisungen zu seiner Verwendung finden Sie in der Dokumentation und der Online-Hilfe für die von Ihnen verwendete UNIX-Plattform und -Version.

Das Hilfsprogramm *mtrace* gibt den Multicast-Pfad von einer Quelle zu einem Empfänger an. *mtrace* verwendet eine Tracing-Funktion von Multicast-Routern, die als *mrouted* klassifiziert sind. Der Zugriff auf diese Funktion erfolgt über eine Erweiterung zum Internet Group Management Protocol (IGMP). Das Hilfsprogramm *mtrace* führt eine Hop-by-Hop-Trace-Abfrage entgegen der angegebenen Pfadrichtung vom *Empfänger* zur *Quelle* durch. Dabei sammelt es Hop-Adressen, führt Paketzählungen durch, protokolliert Routing-Fehler und gibt die Ergebnisse an den Anforderer zurück.

Die exakte Syntax finden Sie auf der Hauptseite für die von Ihnen verwendete UNIX-Plattform und -Version. Die Syntax sieht etwa wie folgt aus:

Beispiel

```
mtrace [ -g Gateway ] [ -i IF_Adresse ] [ -l ] [ -M ] [ -m Max_Hops ]
      [ -n ] [ -p ] [ -q nqueries ] [ -r Responder-Ziel ] [ -s ] [ -S Stat_Int
]
      [ -t ttl ] [ -v ] [ -w Wartezeit ] Quelle [ Empfänger ] [ Gruppe ]
```

Der einzige erforderliche Parameter ist der Hostname und die Adresse der *Quelle*.

Hinweis zu den Hilfsprogrammen von UNIX und Microsoft: Die meisten Diagnose- und Konfigurationsdienstprogramme sind hardware-spezifisch. Das hier erläuterte Hilfsprogramm von UNIX oder Microsoft ist im Lieferumfang bestimmter Versionen der entsprechenden Betriebssysteme enthalten. Weitere Informationen und Support zu Hilfsprogrammen für Computer, Router, Switches und Netzwerke erhalten Sie in der jeweiligen Online-Hilfe und Dokumentation des Anbieters.

Business Process Views-Installation schlägt fehl

Symptom:

Meine Installation der Business Process Views ist mit Repository- und SQL-Fehlern fehlgeschlagen.

Lösung:

Bei nicht englischsprachigen Standorten kann das Dezimalzeichen Probleme bei der Installation oder Aktualisierung der Business Process Views verursachen. Die folgenden Lösungen gelten für Computer, auf denen sowohl CA ITCM als auch Data Transport Service installiert ist. Verwenden Sie als Dezimalzeichen den Punkt, oder ändern Sie andere standortspezifische Einstellungen (laut folgenden Anweisungen). Führen Sie dann das Programm "dtsbpv" erneut aus, und prüfen Sie, ob die Data Transport-3D-Symbole ordnungsgemäß installiert wurden.

Windows

Wenn Sie als Dezimalzeichen ein Komma (,) und keinen Punkt (.) verwenden und das Network Business Views-Installationsprogramm auf Ihrem Computer ausführen, werden den Objekten und Klassen in der MDB keine Data Transport-3D-Symbole hinzugefügt, und SQL-Fehler treten auf. Um diese Probleme zu beheben, wählen Sie auf Windows-Computern "Start", "Einstellungen" und "Systemsteuerung" aus und klicken dann auf "Ländereinstellungen". Wählen Sie im Dialogfeld "Ländereinstellungen" als Dezimaltrennzeichen den Punkt (.) aus.

Linux (oder Linux/UNIX)

Wenn Sie als Dezimalzeichen ein Komma (,) und keinen Punkt (.) verwenden und das Network Business Views-Installationsprogramm auf Ihrem Computer ausführen, können Repository- und SQL-Fehler auftreten. In der Dokumentation zu Ihrem Betriebssystem finden Sie Anweisungen, wie Sie den Punkt als Dezimalzeichen festlegen oder andere standortspezifische Einstellungen ändern können.

DFÜ-Unterstützung funktioniert nicht

Symptom:

Wie verwende ich DTS mit einem Modem und einem DFÜ-Dienstanbieter?

Lösung:

DTS verwendet ein Punkt-zu-Punkt-Protokoll, um eine IP-Verbindung über eine DFÜ-Verbindung herzustellen. TCP wird dann über die Punkt-zu-Punkt-Verbindung verwendet. Hierfür muss ein PPP-Anbieter für den Initiator- und den Responder-Computer verfügbar sein.

Technischer Support

Wenn Sie Hilfe benötigen, wenden Sie sich an den Technischen Support unter <http://ca.com/worldwide>.

Anhang A: Befehle

Dieser Anhang enthält zusammenfassende Informationen zu CLI-Befehlen für DTS-Übertragungen.

Hinweis: Detaillierte Informationen finden Sie im *Referenzhandbuch für DTSCLI-Befehle*.

Dieses Kapitel enthält folgende Themen:

[Befehle "dtacli" und "dtscli"](#) (siehe Seite 95)

[Befehl "dtscli" – Verwalten von Datenübertragungen](#) (siehe Seite 95)

Befehle "dtacli" und "dtscli"

Die folgende Tabelle enthält eine kurze Beschreibung der Befehle "dtacli" und "dtscli":

Befehl	Beschreibung
dtacli	Mit dem Befehl "dtacli" können Sie umfassende Punkt-zu-Viele- oder Punkt-zu-Punkt-Übertragungen sowie direkte Übertragungen zwischen Agenten, also ohne einen Transfer Object Server oder Network Object Server, durchführen.
dtscli	Der Befehl "dtscli" führt alle Aufgaben von "dtacli" durch und enthält darüber hinaus Funktionen wie HTTP-Übertragungen (Internet-Downloads), die Erstellung und Bearbeitung von Übertragungsjobs und Zeitplänen sowie die Übernahme von Eingaben aus einer Befehlsdatei.

Weitere Informationen:

[dtscli \(Befehl\)](#) (siehe Seite 13)

Befehl "dtscli" – Verwalten von Datenübertragungen

Der Befehl "dtscli" verwaltet Datenübertragungen, Übertragungsjobs und Zeitpläne. DTSCLI fasst verwandte Argumente aufgrund der großen Anzahl von Befehlszeilenargumenten in Gruppen zusammen. Argumente werden in der Befehlszeile von link nach rechts angegeben und bezüglich der zuletzt angegebenen Argumentengruppe interpretiert.

Dieser Befehl hat das folgende Format:

```
dtscli [-tos Parameter]  
      [-sos Parameter]  
      [-transfer Parameter]  
      [-job Parameter]  
      [-schedule Parameter]  
      [-mode Modus]  
      [-log Parameter]  
      [-c Kommentar-Zeichenfolge]  
      [@Dateiname]  
dtscli [-agent Parameter]  
      [-log Parameter]  
      [-c Kommentar-Zeichenfolge]  
      [@Dateiname]  
dtscli -help [Gruppe [Argument]]  
dtscli -version
```

-tos

(Optional) Gibt den Speicherort des Transfer Object Server (TOS) sowie alle zur Herstellung einer Verbindung notwendigen Benutzeranmeldeinformationen an.

-sos

(Optional) Gibt den Speicherort des Schedule Object Server (SOS) sowie alle zur Herstellung einer Verbindung notwendigen Benutzeranmeldeinformationen an.

-transfer

(Optional) Erstellt, löscht und ruft den Status der Übertragungsobjekte ab.

-job

(Optional) Erstellt, löscht und ruft andere Methoden für Übertragungsjobobjekte auf.

-schedule

(Optional) Erstellt, löscht und ruft andere Methoden für Zeitplanobjekte auf.

-mode

(Optional) Gibt den Modus der Objektlebenszeit an, der steuert, ob durch DTSCLI erstellte Übertragungen nach der Erstellung aktiviert werden und ob sie dann nach Abschluss der Übertragung gelöscht werden.

-log

(Optional) Gibt an, ob die Übertragungen synchron oder asynchron aktiviert werden und welche Protokollierungsebene erforderlich ist.

-c

(Optional) Gibt einen Kommentar an.

Standard: Keine

@Dateiname

(Optional) Gibt den vollständigen Pfad der Befehlsdatei an, die gelesen und als Eingabe verwendet werden soll.

-agent

(Optional) Führt Agent-zu-Agent-Übertragungen durch.

-help

Zeigt Hilfe zur dtscli-Befehlszeilenschnittstelle an.

-version

Zeigt Versionsinformationen zur dtscli-Befehlszeilenschnittstelle an.

Beispiel: Erstellen grundlegender Übertragungsvorgänge

Im folgenden Beispiel werden ein Übertragungsobjekt und ein Übertragungsjobobjekt erstellt. Danach wird die Übertragung zum Übertragungsjob hinzugefügt, der Übertragungsjob ausgeführt und das Übertragungsobjekt sowie das Übertragungsjobobjekt gelöscht. Die Argumente ipath und rpath geben den vollständigen Dateipfad auf dem Initiator bzw. dem Responder an. In diesem Beispiel wird davon ausgegangen, dass sich der TOS auf dem lokalen Rechner befindet und sowohl der TOS als auch die zwei DTS-Agenten im stillen Modus verwendet werden.

```
dtscli -transfer ipath=jupiter::c:\data\03105.dat  
rpath=neptune::c:\data\jupiter\03105.dat
```


Anhang B: Unterstützung für externe Filter

Wie bereits erwähnt, unterstützt DTS externe Paketfilter und externe Dateifilter.

In früheren Versionen von DTS konnte mit dem Parameter "OUTPUT=" für externe Dateien angegeben werden, ob Ihr externer Filter eine Ausgabedatei erstellt oder keine Ausgabe erzeugt. Mit DTS wurde dieser Parameter erweitert, so dass mit dem externen Filter nun auch ein Ausgabeverzeichnis erstellt werden kann.

Weitere Informationen:

[Filter](#) (siehe Seite 35)

Terminologieglossar

Anwendung

Eine *Anwendung* ist eine Software, zum Beispiel Microsoft Word.

Anwendungsvirtualisierung

Anwendungsvirtualisierung ist die Verkapselung einer Anwendung, indem sie vom zu Grunde liegenden Betriebssystem abgetrennt wird, unter dem es ausgeführt wird. In der Laufzeit wird die Anwendung dazu gebracht, so zu handeln, als ob sie direkt mit dem ursprünglichen Betriebssystem und allen davon verwalteten Ressourcen verbunden ist, aber in Wirklichkeit ist es nicht so.

Common Configuration Enumeration (CCE)

Common Configuration Enumeration (CCE) ist einer der SCAP-Standards. Er enthält Standard-IDs und ein Wörterbuch zu sicherheitsbezogenen Systemkonfigurationsproblemen. Eine Rollendefinition in einem SCAP-Datenstrom kann Referenzen zu einer oder mehreren CCE-IDs, enthalten, was angibt, dass die Regel eine spezifische CCE-Konfigurationsanweisung oder eine Konfigurationskontrolle darstellt. Weitere Informationen erhalten Sie unter <http://cce.mitre.org/>.

Common Platform Enumeration (CPE)

Common Platform Enumeration (CPE) ist einer der SCAP-Standards. Er enthält Standard-IDs und ein Wörterbuch zu Plattform- und Produktnamen. Einige Elemente in XCCDF-Dateien, zum Beispiel, können auf die Anwendung ausschließlich auf bestimmten Plattformen beschränkt werden, und die erfolgt mittels CPE-IDs. Weitere Informationen erhalten Sie unter <http://cpe.mitre.org/>.

Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE) ist ein Wörterbuch gebräuchlicher Begriffe (CVE-Identifikatoren) für öffentlich bekannte Sicherheitslücken. Diese Identifikatoren erleichtern das Austauschen von Daten über mehrere Netzwerk-Sicherheitsdatenbanken und Hilfsprogramme hinweg. CVE ist nur eine der in SCAP verwendeten Komponenten. Weitere Informationen finden Sie unter <http://cve.mitre.org/>.

Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) ist einer der SCAP-Standards. Es enthält Standards für die Übermittlung und die Bewertung der Auswirkungen von Sicherheitslücken. Weitere Informationen erhalten Sie unter <http://www.first.org/cvss/index.html>.

Connectors

Connectors sind die Verknüpfungen von Produkten, die Connector-Daten für externe Produkte oder *Domänen-Manager* verarbeiten. Jeder Connector ruft Informationen seines Domänen-Managers ab und übermittelt die Informationen über das Connector-Framework an das Consumer-Produkt zur Anzeige und Analyse. Connectors können auch eingehende Vorgänge für Daten im Quell-Domänen-Manager veranlassen, beispielsweise Objekterstellung. Connectors verwenden ein vereinheitlichtes Connector-Framework, um die Integration mit mehreren Produkten zu ermöglichen, die Sie verwenden.

Desktop-Aktualisierung

Bei der *Desktop-Aktualisierung* wird der virtuelle Desktop in den Originalstatus zurückversetzt. Verknüpfte Klone verfolgen Änderungen für den virtuellen Rechner mit dem Klon nach. Um die Speicherzuweisungen mit dem Klon zu steuern, stellt VMware View den Aktualisierungsvorgang bereit, der den Klon auf die Baseline zurücksetzt und alle für Änderungsnachverfolgungen bereitgestellten Deltas freigibt. Demnach gehen alle auf dem Systemdatenträger seit der Erstellung des Klons oder seiner letzten Aktualisierung oder Neuzusammenstellung gespeicherten Informationen verloren. Im Gegensatz zur Desktop-Neuzusammenstellung wird dasselbe Golden Template wie vor dem Aktualisierungsvorgang verwendet.

Desktop-Neuzusammenstellung

Die *Desktop-Neuzusammenstellung* ist ein Prozess, bei dem dem virtuellen Desktop eine neues Golden Template zugewiesen wird. Betriebssysteme und Anwendungen müssen während ihrer Lebenszeit verwaltet werden, um Probleme mittels Hotfixes oder Services Packs zu beheben oder neue Funktionen durch neue Versionen bereitzustellen. Für verknüpfte Klone bedeutet dies, dass das Master-Image oder das Golden Template aktualisiert werden muss. Sobald die Aktualisierungen abgeschlossen sind, wird der verknüpfte Klon neu zusammengestellt und wird aktiv. Während der Operation der Neuzusammenstellung werden die entsprechenden verknüpften Klone mit dem neuen Golden Template verknüpft und aktualisiert.

Durch Staging bereitgestelltes Image der virtuellen Anwendung

Ein *zwischen gespeichertes Image einer virtuellen Anwendung* ist das Image einer virtuellen Anwendung, das im File System eines Computers entdeckt wurde.

Eigenständige Umgebung

Als *eigenständige Umgebung* wird eine Umgebung bezeichnet, in der die Benutzer des Host- und des Viewer-Computers sämtliche Einstellungen, Eigenschaften und die Lizenzierung der CA ITCM-Remote Control-Komponente lokal verwalten. Eingerichtet wird sie mit Hilfe einer eigenständigen Agenten-Installation. Wenn Sie die Installation manuell ausführen möchten, muss das Setup für den RC-Agenten direkt aufgerufen werden.

Eigenständige virtuelle Anwendung

Eine *eigenständige virtuelle Anwendung* ist eine virtuelle Anwendung, die so zur Verfügung gestellt worden ist, dass das als Quelle verwendete Image der virtuellen Anwendung auf dem System beherbergt wird, auf dem es zur Verfügung gestellt worden ist.

eXtensible Configuration Checklist Description Format (XCCDF)

eXtensible Configuration Checklist Description Format (XCCDF) ist eine Spezifikationssprache, die zum Schreiben von Sicherheits-Checklisten, Benchmarks und ähnlichen Arten von Dokumenten verwendet wird. Ein XCCDF-Dokument stellt eine strukturierte Sammlung von Sicherheitskonfigurationsregeln für eine Gruppe von Zielcomputern dar. Die Spezifikation unterstützt den Austausch von Informationen, die Generierung von Dokumenten, die Anpassung an Organisationen und Situationen, die automatisierte Compliance-Kontrolle sowie die Bewertung der Compliance. Weitere Infos finden Sie unter <http://nvd.nist.gov/xccdf.cfm>.

Federal Information Processing Standard (FIPS)

Federal Information Processing Standard (FIPS) ist ein Sicherheitsstandard, der vom NIST herausgegeben und genehmigt wird. Es gibt an, welche Sicherheitsanforderungen von einem kryptographischen Modul erfüllt werden müssen, die innerhalb eines Sicherheitssystems verwendet werden, das vertrauliche, aber nicht geheime, Information schützt.

FIPS-bevorzugt

FIPS-bevorzugt ist eine Betriebsart für CA ITCM, in der Großteil der kryptographischen Operationen FIPS-kompatibel sind, wenige Verschlüsselungen werden im früheren Format belassen. In diesem Modus ist CA ITCM rückwärts-kompatibel mit den früheren Versionen von CA ITCM.

FIPS-kompatible Kryptographie

FIPS-kompatible Kryptographie bezieht sich auf die Verwendung von FIPS 140-2-zertifizierten Modulen, FIPS-anerkannt, und von FIPS zugelassene Verfahren und Algorithmen für Kryptographie.

FIPS-zertifiziertes Kryptographiemodul

FIPS-zertifiziertes Kryptographiemodul bezieht sich auf das Modul "RSA CryptoC BSAFE", das für FIPS 140-2-zertifiziert ist.

Flüchtige Klone

Flüchtige Klone sind virtuelle Desktops aus dem flüchtigen Pool von VMware View-Benutzerdaten, die vorübergehend integriert sind. Sobald ein Benutzer sich abmeldet, wird der Klon aktualisiert, und alle Benutzerdaten auf dem Systemdatenträger gehen verloren.

Gast

Ein *Gast* in der Terminologie der generischen Plattformvirtualisierung ist der virtuelle Rechner und das Gastbetriebssystem.

Gastbetriebssystem

Das *Gastbetriebssystem* führt das Betriebssystem, das in einem virtuellen Rechner ausgeführt wird.

Gehostete virtuelle Umgebung

Eine *gehostete virtuelle Umgebung* ist die Virtualisierungs-Software, die zusätzlich zu einem Hostbetriebssystem, das heißt, dem physischen Rechner, dem Host-BS, und dem Hypervisor ausgeführt wird.

Gestreamte virtuelle Anwendung

Eine *gestreamte virtuelle Anwendung* ist eine virtuelle Anwendung, die derart zur Verfügung gestellt worden ist, dass das als Quelle verwendete Image der virtuellen Anwendung auf einem anderen Remote- System beherbergt wird, als dem System ist, in dem es zur Verfügung gestellt wird.

Gestreamtes Image der virtuellen Anwendung

Ein *gestreamtes Image der virtuellen Anwendung* ist das Image einer virtuellen Anwendung, das als über das Netzwerk für einen Computer verfügbar entdeckt wurde. Die Entdeckung des gestreamten Image einer virtuellen Anwendung wird üblicherweise nur möglich sein, wenn die virtuellen Anwendungen sich innerhalb des zur Verfügung gestellten Images befinden.

Golden Template

In der CA ITCM-Terminologie ist das *Golden Template* der virtuelle Rechner, von dem aus die virtuellen Desktops geklont werden.

Host

Ein *Host* in der Terminologie der generischen Plattformvirtualisierung ist der physische Rechner, das Host-Betriebssystem und der Hypervisor.

Host-Betriebssystem

Das *Hostbetriebssystem* ist das Betriebssystem, das auf einem physischen Rechner ausgeführt wird.

Host-Cluster

Der *Hostcluster* ist die Gesamtmenge der Datenverarbeitungs- und Speicherressourcen einer Gruppe von Hosts, die zum Teil oder insgesamt das gleiche Netzwerk und den gleichen Speicher gemeinsam nutzen.

Hypervisor

Der *Hypervisor* ist die Virtualisierungs-Schicht, die physische Hardware im Namen des Gastbetriebssystems simuliert. Dieser Begriff ist synonym zu Virtual Machine Monitor (VMM).

Image der virtuellen Anwendung

Ein *Image der virtuellen Anwendung* enthält eine oder mehrere virtuelle Anwendungen, die in einer Datei gespeichert wurden, möglicherweise mit einem Set unterstützender Metadateien.

Image-Definition der virtuellen Anwendung

Eine *Image-Definition der virtuellen Anwendung* bezeichnet die "Spur" für die Entdeckung des Image einer virtuellen Anwendung. Um ein Bild zu entdecken, dass eine oder mehrere eingeschlossene virtuelle Anwendungen enthält (in ihm gespeichert), müssen normale Softwaresignaturen mit der Image-Definition der virtuellen Anwendung verknüpft werden.

Instanz-Softwarestatusdatenbank

Die *Instanz-Softwarestatusdatenbank* ist ein Bestandteil der Softwarestatusdatenbank, die den Verlauf sämtlicher durch den Agent ausgeführten Softwarejobs enthält, die auf einem Nicht-Golden-Template-System ausgeführt wurden, d. h. alle Klone des Golden Template.

Konfigurationsansicht

Eine *Konfigurationsansicht* ist eine angepasste Windows-Benutzeroberfläche, auf der Sie Konfigurationsrichtlinien für bestimmte Komponenten oder Funktionen bearbeiten können. In den Konfigurationsansichten werden die relevanten Richtlinien für eine Komponente oder für eine Funktion unabhängig davon aufgeführt, an welcher Stelle sie sich tatsächlich in der Hierarchie und in der DSM-Explorer-Baumstruktur befinden.

Master-vDisk

In Citrix XenDesktop ist eine *Master-vDisk* die initiale vDisk, die vom Golden Template-Computer generiert wird.

Masterzielgerät

In Citrix XenDesktop ist ein *Masterzielgerät* der Basis-Desktop mit dem BS und dem erforderlichen Satz an Anwendungen, von dem eine vDisk generiert wird.

MITRE

Die *MITRE Corporation* ist eine gemeinnützige Organisation, die für Tätigkeiten in öffentlichem Interesse gegründet wurde. MITRE bietet Übersetzungsprogramme, Quellcode, Schemata, und Dateien kostenlos an, damit Einzelpersonen und Organisationen auf sie bauen und sie erweitern können. OVALdi ist ein solches frei erhältliches Übersetzungsprogramm

National Institute of Standards and Technology (NIST)

Das *National Institute of Standards and Technology (NIST)* ist ein nichtregulierendes Bundesamt des US-Handelsministeriums. Aufgabe des NIST ist es, die US-amerikanische Innovation und industrielle Wettbewerbsfähigkeit zu fördern, indem es die Wissenschaft, Standards und Technologie des Messens so fördert, dass die wirtschaftliche Sicherheit und unsere Lebensqualität verbessert werden. Die US-amerikanische nationale Datenbank für Sicherheitslücken, National Vulnerability Database (NVD), die vom NIST betrieben wird, bietet ein Repository und Daten-Feeds mit Inhalten, die SCAP-Standards verwenden. Es ist außerdem das Repository für einige offizielle Daten zu SCAP-Standards. So definiert NIST offene Standards innerhalb des SCAP-Kontextes und definiert die Zuordnungen zwischen den SCAP-Aufzählungsstandards.

Nicht verknüpfte Klone

In VMware View sind *nicht verknüpfte Klone* oder vollständige Klone vollständige Kopien des Master- oder Golden Images. Der Klon enthält eine Kopie des Images, und alle Änderungen am System bei Benutzersitzungen werden in dieser Kopie gespeichert.

Normale Anwendung

Eine *normale Anwendung* ist Anwendungssoftware, die nicht virtualisiert worden ist und die in traditioneller Weise installiert und ausgeführt werden kann. Wenn Versionen, Patches, und Suiten erwähnt werden, handelt es sich um normale Anwendungen.

Nur-FIPS

Nur-FIPS ist eine Betriebsart für CA ITCM, in der nur FIPS-kompatible Kryptographie erlaubt ist. In diesem Modus ist CA ITCM nicht rückwärtskompatibel mit den früheren Versionen von CA ITCM.

Offline-Patching

Mit dem Offline-Patching können Sie Patch-Inhalte und -Dateien remote exportieren und sie mit dem CA Patch Manager ohne Internetzugriff in der CA ITCM-Umgebung importieren.

Offline-RAC

Bei einem *Offline-RAC* handelt es sich um einen RAC-Task (Neuinstallation nach Absturz, Reinstall After Crash), der nicht durch den Manager, sondern durch den Agent gesteuert wird. Virtuelle Desktops werden häufig *erneut erstellt*, das heißt, wenn das Golden Template aktualisiert und die Festplatte zurückgesetzt wird, werden alle Änderungen am virtuellen Desktop seit der vorherigen Zurücksetzung effektiv ungültig gemacht. Bei virtuellen Desktops ist nicht der Manager, sondern der Agent für die Erstellung des RAC-Jobcontainers verantwortlich. Bei einer Datenträgerzurücksetzung initiiert der Agent einen Offline-RAC, um sämtliche Software wiederherzustellen, die für den Agent bereitgestellt wurde.

Open Vulnerability and Assessment Language (OVAL)

Open Vulnerability and Assessment Language (OVAL) ist einer der SCAP-Standards. Es enthält Standard-XML für Testverfahren im Zusammenhang mit sicherheitsrelevanten Softwarefehlern, Konfigurationsproblemen und Patches sowie mit der Weitergabe der Testergebnisse. Alle Regelüberprüfungen in der Checkliste haben die Form von Referenzen zu OVAL-Definitionen, die in OVAL-Dateien aus dem SCAP-Datenstrom enthalten sind. Weitere Informationen erhalten Sie unter <http://oval.mitre.org/>.

Ovaldi

Ovaldi ist ein OVAL-Übersetzungsprogramm, das von der MITRE Corporation entwickelt wurde. Es ist eine frei verfügbare Referenzimplementierung, die erstellt wurde, um zu zeigen, wie Informationen von einem Computer zu Testzwecken erhalten werden können, um die OVAL-Definitionen für diese Plattform zu bewerten und auszuführen und um die Testergebnisse weiterzugeben. Das Übersetzungsprogramm zeigt die Nutzbarkeit der OVAL-Definitionen auf und sorgt für eine korrekte Syntax und die Einhaltung des OVAL-Schemas.

Paket mit eigenständiger virtueller Anwendung

Ein *Paket mit einer eigenständigen virtuellen Anwendung* ist ein Paket mit einer virtueller Anwendung, das verwendet wird, um eine virtuelle Anwendung in eigenständigem Modus zur Verfügung zu stellen.

Paket mit virtueller Anwendung (VAP)

Ein Image einer virtuellen Anwendung, das in ein oder mehr Software Delivery verpackt ist, wird als *virtuelles Anwenderpaket* bezeichnet. Diese Pakete werden verwendet, um virtuelle Anwendungen auf Computern zur Verfügung zu stellen.

Paket zum Streaming der virtuellen Anwendung

Ein *Paket zum Streaming der virtuellen Anwendung* ist ein Paket mit einer virtueller Anwendung, das verwendet wird, um eine virtuelle Anwendung im Streaming- Modus zur Verfügung zu stellen.

Paket zur Bereitstellung der virtuellen Anwendung durch Staging

Ein *Paket zur Bereitstellung der virtuellen Anwendung durch Staging* ist ein Paket mit einer virtuellen Anwendung, das verwendet wird, um das Image der virtuellen Anwendung durch Staging bereitzustellen.

Paketformat

Das *Paketformat* ist eine Eigenschaft eines Softwarepakets. Formate sind "normal" und "virtuell".

Pakettyp

Der *Pakettyp* ist eine Eigenschaft eines Softwarepakets. Derzeitige Typen sind Allgemein, MSI, SXP, PIF und PKG. Paket-Typ wird nicht verwendet oder geändert, um virtuelle Anwendungspakete zu unterstützen.

Partition

Eine *Partition* ist eine isolierte Instanz eines Hostbetriebssystems. Partitionen verwenden normalerweise keine Gastbetriebssysteme, weil sie alle das Betriebssystem des Hosts gemeinsam nutzen.

Partitionierte virtuelle Umgebung

Eine *partitionierte virtuelle Umgebung* ist eine Umgebung, in der mehrere Instanzen des Host-Betriebssystems isoliert auf dem gleichen physischen Rechner ausgeführt werden können. Streng genommen handelt es sich nicht um eine Virtualisierungs-Technologie, aber sie wird verwendet, um die gleichen Probleme zu lösen.

Permanente Klone

Permanente Klone sind virtuelle Desktops des permanenten Pools, die in ihrer Form bestehen bleiben, nachdem sich der Benutzer abgemeldet hat, bis sie aktualisiert oder erneut erstellt werden. VMware View bietet integrierte getrennte Geräte für System- und Benutzerdaten mit den permanenten Klonen. Auf dem Benutzerdatengerät gespeicherte Informationen bleiben von jeder Aktualisierung oder Neuzusammenstellung unberührt, während Änderungen am Systemdatenträger verloren gehen.

Plattformvirtualisierung

Plattformvirtualisierung ist die Verkapselung von Computern oder Betriebssystemen, indem ihre physischen Merkmale vor den Benutzern verborgen werden und die Datenverarbeitungsplattform in der Laufzeit nachgeahmt wird.

Replikation

Bei der *Replikation* handelt es sich um einen Engine-Task zum Ausführen der Datenreplikation vom Domänen-Manager zum Enterprise-Manager und umgekehrt.

Sandkasten

Ein Sandkasten ist die Laufzeitumgebung einer Anwendung, die die Anwendung vom Betriebssystem und den Ressourcen des Computers sowie von anderen Anwendungen auf dem Computer isoliert. Der Grad der Isolation wird üblicherweise festgelegt, um der Anwendung einen beschränkten Zugriff auf Ressourcen des Betriebssystems zu erlauben, z. B. auf den Ordner "Eigene Dateien" .

Scalability-Server

Ein *Scalability-Server* ist der zentrale Server, um eine geographische Skalierbarkeit für Management-Tasks zu ermöglichen. Es handelt sich um einen verteilten Prozess, der die primäre Schnittstelle des Agenten ist.

SCAP-Datenstrom

Ein SCAP-Datenstrom besteht aus Sicherheits-Checklisten in automatischen XML-Formaten, Aufzählungen zu Sicherheitslücken und Produktnamen sowie Zuordnungen zwischen den Aufzählungen. Ein SCAP-Datenstrom besteht aus den folgenden XML-Dateien:

- Eine XCCDF-Datei
- Eine oder mehrere OVAL-Dateien
- (Optional) Eine CPE-Wörterbuchdatei

Schemazuordnung

Eine *Schemazuordnung* ist eine Zuordnung der mit Datenobjekten wie Benutzern, Computern und Gruppen verknüpften Attributnamen, die in einem externen Verzeichnis verwendet werden, zu den Attributnamen, die von den entsprechenden CA ITCM-Objekten verwendet werden. Der feste Satz und der Standardsatz der DSM-Attributnamen werden zur Abfrage von Verzeichnissen und zur Formulierung komplexer Abfragen und Berichte verwendet.

Security Content Automation Protocol (SCAP)

Das *Security Content Automation Protocol (SCAP)*, "S Cap" ausgesprochen, ist eine Methodik für die Verwendung von Standards wie XCCDF, CCE, CVE, CVSS, CPE und OVAL für automatisches Sicherheitslückenmanagement und die Bewertung der Einhaltung von Richtlinien (z. B. FISMA-Compliance). Genauer betrachtet SCAP ist eine Suite ausgewählter offener Standards, die Softwarefehler, sicherheitsrelevante Konfigurationsprobleme und Produktnamen aufzählen, und die Maßsysteme, um das Vorkommen von Sicherheitslücken festzustellen sowie Mechanismen, die die Ergebnisse dieser Messungen einordnen, um die Auswirkungen der entdeckten Sicherheitsprobleme zu beurteilen, enthalten. SCAP definiert, wie diese Standards kombiniert werden. Die nationale Datenbank für Sicherheitslücken stellt ein Repository und Daten-Feeds mit Inhalten, die die SCAP-Standards verwenden, zur Verfügung. Weitere Infos finden Sie unter <http://nvd.nist.gov/>.

Softwaresignatur

Eine *Softwaresignatur* definiert die Attribute einer Softwareanwendung, z. B. den Dateinamen der Hauptprogrammdatei, andere dazugehörige Dateien, den Größenbereich, Versionsbereich sowie das Erstellungs- und Änderungsdatum der Software. Alle diese Attribute einer Softwaresignatur dienen zur eindeutigen Identifikation einer Anwendung. Softwaresignaturen in Asset Management werden als Softwaredefinitionen erstellt. Sie können Softwaredefinitionen für ein Produkt, eine Version, einen Patch, eine Suite, eine Suite-Komponente oder ein Image der virtuellen Anwendung erstellen. Standardmäßig enthält Asset Management vordefinierte Softwaresignaturen für die branchenweit am häufigsten verwendeten Softwareprogramme.

Softwaretyp

Der *Software-Typ* ist eine Eigenschaft einer Softwaredefinition. Derzeitige Typen schließen Suite, Produkt, Version, Patch, und Image der virtuellen Anwendung ein.

Standorterkennung

Mit der *Standorterkennung* kann der DSM-Agent auf einem Computer den Standort des Computers feststellen.

Systemeigene virtuelle Umgebung

Eine *systemeigene virtuelle Umgebung* ist die Virtualisierungs-Software, die direkt auf dem physischen Rechner ausgeführt wird oder die als Host-Betriebssystem handelt oder auftritt (oft minimal), das heißt, der Rechner und der Hypervisor. Ein synonyme Begriff ist "Bare Metal-Umgebung".

vDisk

In Citrix XenDesktop ist eine *vDisk* oder ein virtueller Datenträger prinzipiell eine Image-Datei mit dem BS und dem erforderlichen Satz an Anwendungen.

Verknüpfte Klone

In VMware View verweisen *verknüpfte Klone* eines Master- oder Golden Images nur auf das Master- oder Golden Image, aber sie enthalten es nicht. Änderungen, die bei Benutzersitzungen am System vorgenommen werden, werden nicht im Master-Image gespeichert, sie werden nur in Delta-Dateien mit dem Klon beibehalten.

virtuelle Anwendung (VA)

Eine *virtuelle Anwendung* ist Software, die virtualisiert worden ist.

Virtuelle Festplatte

Eine *virtuelle Festplatte* ist ein Set von Dateien, die ein Dateisystem bildet, das als physischer Datenträger im Gastbetriebssystem erscheint.

Virtuelle Version

Eine *virtuelle Version* ist das virtuelle Äquivalent zur normalen Version und hat die gleiche grundlegende Bedeutung. Der Begriff wird verwendet, wenn man über Software-Inventar für virtuelle Anwendungen berichtet (nicht Images der virtuellen Anwendung). Beachten Sie, dass eine zur Verfügung gestellte virtuelle Anwendung entweder ein durch Staging bereitgestelltes oder ein per Datenstrom übertragenes Image einer virtuellen Anwendung als Quelle verwenden kann. Die virtuellen Anwendungen, die im Images der virtuellen Anwendung enthalten sind können als durch Staging bereitgestellt, aber nicht zur Verfügung gestellt angesehen werden.

Virtueller Desktop flüchtig verknüpfter Klone

Ein *virtueller Desktop flüchtig verknüpfter Klone* ist ein virtueller Rechner, der bei jeder Benutzeranmeldung aktualisiert oder erneut erstellt wird, und zwar ohne Persistenz für benutzerdefinierte installierte Anwendungen, Personalisierung usw.

Virtueller Desktop permanent verknüpfter Klone

Ein *virtueller Desktop permanent verknüpfter Klone* ist ein virtueller Rechner, der für einen bestimmten Benutzer dediziert ist, und der Benutzer kann das Hinzufügen bestimmter Software anfordern, Einstellungen anpassen usw. Die benutzerdefinierte Umgebung des Benutzers wird bei jeder Anmeldung wiederhergestellt. Dies wird so beibehalten, bis der virtuelle Desktop aktualisiert oder erneut erstellt wird. Zu diesem Punkt gehen alle auf dem Systemdatenträger installierten Softwareprodukte verloren.

Virtueller Desktop permanenter, nicht verknüpfter Klone

Ein *virtueller Desktop permanenter, nicht verknüpfter Klone* ist ein virtueller Rechner, der für einen bestimmten Benutzer dediziert ist, und er wird dem Benutzer bei jeder Anmeldung mit den entsprechenden benutzerdefinierten installierten Anwendungen, Benutzereinstellungen, Daten usw. angezeigt.

Virtueller Patch

Ein *virtueller Patch* ist das virtuelle Äquivalent zu einem normalen Patch und hat die gleiche grundlegende Bedeutung. Der Begriff wird verwendet, wenn man über Software-Inventar für virtuelle Anwendungen berichtet (nicht Images der virtuellen Anwendung).

Virtueller Rechner (VM)

Ein *virtueller Rechner* ist eine isolierte virtualisierte Umgebung, die einen Computer simuliert. Der virtuelle Rechner schließt definitionsgemäß das Gastbetriebssystem nicht ein.

Virtuelles Image

A *virtuelles Image* ist eine Datei oder Set von Dateien, die die vollständige Definition eines virtuellen Rechners, einschließlich seiner Hardware-Spezifikationen und virtuellen Festplatten enthalten. Es ist die Darstellung des Host-Dateisystems eines Gastes. Ein virtuelles Image kann online oder offline sein, je nach dem Laufstatus des virtuellen Rechners, den es abbildet.

XCCDF-Profil

Ein *XCCDF-Profil* ist eine Richtlinie, die auf den Zielcomputer angewendet oder mit der Konfiguration des Zielcomputers verglichen wird. Die XCCDF-Datei für jeden SCAP-Datenstrom definiert eine Liste der unterstützten Profile. Die XCCDF-Datei muss mindestens ein XCCDF-Profil enthalten, das angibt, welche spezifischen Regeln für die Überprüfung eines bestimmten Systemtyps verwendet werden. Sie können unterschiedliche XCCDF-Profile für jede anwendbare Betriebsumgebung, in der das System implementiert werden kann, erstellen.

Zentral verwaltete Hostumgebung

Bei einer *zentral verwalteten Hostumgebung* ist entweder ein Enterprise-Manager oder ein Domänen-Manager von Remote Control für die Konfiguration der Hosts sowie für die Authentifizierung von Viewer-Verbindungen verantwortlich. Außerdem verwaltet dieser Server die Adressbücher, die die Benutzer zur Hostsuche verwenden.

Zentral verwaltete Umgebung

In einer *zentral verwalteten Umgebung* steuert der Remote Control-Domänen-Manager die Hosteinstellungen durch Computerrichtlinien, Elemente im globalen Adressbuch (GAB), Lizenzierung des Agenten auf der Domäne und Benutzerberechtigungen. Dies ist die Standardeinstellung für CA IT Client Manager.

Zur Verfügung gestellte Anwendung

Eine *zur Verfügung gestellte Anwendung* ist eine Anwendung (normal oder virtuell), die für die Ausführung auf einem Zielcomputer verfügbar gemacht worden ist. Die Anwendung muss nicht lokal "installiert werden", um sie als zur Verfügung gestellt zu behandeln.

Zustandsüberwachung

Mithilfe der *Zustandsüberwachung (Health Monitoring, HM)* können Sie Alarme konfigurieren, Grenzwerte festlegen und den Gesamtzustand der CA ITCM-Infrastruktur überwachen.