Das Stopfen der Lücken, die Azure AD Connect in Ihrer Notfallwiederherstellungsstrategie hinterlässt

Ihre Nur-Cloud-Objekte und -Attribute werden von Ihrem lokalen Sicherungs- und Wiederherstellungsschema nicht erfasst.

EINFÜHRUNG

Wenn Ihre Organisation über eine hybride Active Directory-Umgebung (AD) verfügt oder darüber nachdenkt, zu einer solchen zu wechseln, sind Sie nicht allein. Nach Angaben von Microsoft verfügen 75 Prozent der Kunden mit mindestens 500 Benutzern über eine hybride AD-Umgebung: Das lokale AD bleibt die primäre Authentifizierungs- und Autorisierungsquelle, und dieses lokale AD wird mithilfe von Azure AD Connect zum Azure AD synchronisiert[1]. Benutzer werden mit lokalen Benutzerinformationen für Cloud-Anwendungen authentifiziert und alles wird von der lokalen Sicherungs- und Wiederherstellungslösung geschützt. Was ist nun daran auszusetzen?

Leider schwimmt in der Suppe ein ziemlich dickes Haar. Unsere lokale Lösung ist leider nicht in der Lage, alles zu sichern und wiederherzustellen. Tatsächlich ist es praktisch unmöglich, Office 365 oder Azure auszuführen, ohne irgendwelche Nur-Cloud-Objekte zu erstellen. Da die Azure AD Connect-Synchronisierung in den meisten Fällen eine Einbahnstraße vom lokalen AD zu Azure AD ist, werden diese nur in der Cloud vorhandenen Objekte nicht von Ihren lokalen Datensicherungs- und Wiederherstellungstools erfasst. Darüber hinaus unterliegt die native Option – das Wiederherstellen von Cloud-Objekten aus dem Papierkorb – schmerzlichen Einschränkungen. So bleibt in der Wiederherstellungsstrategie für Ihre Unternehmensdaten eine kritische Lücke.

Dieses Whitepaper erörtert dieses Problem und bietet eine Lösung an. Wir beschäftigen uns damit, wie eine hybride AD-Umgebung funktioniert, wir erläutern die Arten von Nur-Cloud-Objekten und -Attributen und ihren Zweck und behandeln die Einschränkungen nativer Tools bei deren Wiederherstellung. Dann erläutern wir, wie Sie mithilfe von Lösungen von Quest® die von Ihnen benötigte Sicherung, Wiederherstellung und Notfallwiederherstellung erreichen.

1 Simons, Alex, "Best way to connect to Office 365 and Azure AD (latest data) + Azure AD Connect Momentum," Microsoft Enterprise Mobility + Security Blog, Januar 2016, https://cloudblogs.microsoft.com/enterprisemobility/2016/01/05/best-way-to-connect-to-office-365-and-azure-ad-latest-data-azure-ad-connect-momentum/

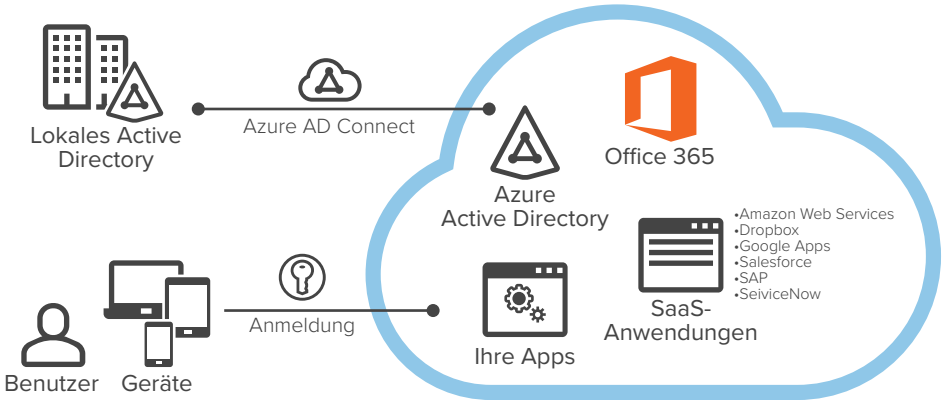

Abbildung 1. Viele Organisationen verbinden ihre lokale Active Directory-Umgebung über Azure AD Connect mit der Microsoft Azure-Cloud.

Wenn wir unsere Kunden fragen, wie viele Nur-Cloud-Objekte und -Attribute bei ihnen auftreten, sagen Sie häufig, sie wüssten es nicht.

DIE ANATOMIE EINER HYBRIDEN ACTIVE DIRECTORY-UMGEBUNG

In den meisten Organisationen mit einer hybriden AD-Umgebung ist das lokale AD die primäre Authentifizierungs- und Autorisierungsquelle, und das lokale AD wird mithilfe von Azure AD Connect mit Azure AD synchronisiert. Wie in Abbildung 1 dargestellt, werden Benutzer mit lokalen Benutzerinformationen für Office 365 sowie für benutzerdefinierte Cloud-Anwendungen und gängige SaaS-Apps (Storage-as-a-Service, Speicherdienste) wie Dropbox, Google Apps und Amazon Web Services (AWS) authentifiziert.

WAS DER SYNCHRONISIERUNG ÜBER AZURE AD CONNECT FEHLT

Für die meisten Kunden verläuft die Synchronisierung nur in eine Richtung: vom lokalen AD zum Azure AD. In der Cloud erstellte Objekte und Attribute werden normalerweis nicht zum lokalen AD zurücksynchronisiert. Das bedeutet, dass sie von den lokalen Sicherungs- und Wiederherstellungslösungen nicht erfasst werden. Wenn Organisationen die Write-Back-Funktion für die Synchronisierung in beiden Richtungen aktivieren, besteht sogar das Risiko, dass noch mehr Objekte in ihrem Azure AD von ihrem Sicherungs- und Wiederherstellungsschema nicht erfasst werden.

Wenn wir unsere Kunden fragen, wie viele Nur-Cloud-Objekte und -Attribute bei ihnen auftreten, sagen Sie häufig, sie wüssten es nicht. Es folgen die am weitesten verbreiteten Arten von Nur-Cloud-Elementen, die für die lokale Sicherung und Wiederherstellung unsichtbar sind, und die Herausforderungen im Zusammenhang mit deren Wiederherstellung in der Cloud mithilfe von nativen Tools.

Nur-Cloud-Attribute

Während die meisten Azure AD-Objekte vom lokalen AD synchronisiert werden, verfügen diese oft über zusätzliche Attribute, die nur in der Cloud vorhanden sind. Dazu zählen:

- **Office 365-Lizenztyp –** Jeder Azure AD-Benutzer verfügt über einen Office 365-Lizenztyp, der die Funktionen bestimmt, die dem Benutzer zur Verfügung stehen.
- **Erweiterungsattribute –** Azure AD erlaubt auch das Erstellen von neuen Attributen für Benutzer, Gruppen und einige weitere Objekte. Finanzdienstleister stellen in Azure z. B. Handelsapplikationen bereit und erstellen ein Erweiterungsattribut, das den Zugriff darauf steuert.

Wenn ein Benutzerobjekt mit einem oder mehreren Nur-Cloud-Attributen gelöscht wird, könnte das Benutzerobjekt im lokalen AD wiederhergestellt und mit Azure AD Connect wieder zu Azure AD zurücksynchronisiert werden, aber die Nur-Cloud-Attribute wären verloren und der Benutzer hätte keinen Zugriff mehr. Wenn z. B. ein Benutzer ohne Lizenztyp-Attribut wiederhergestellt wird, könnte er auf keine Office 365-Anwendung mehr zugreifen. Und Sie müssen sich beeilen, das Attribut wiederherzustellen, bevor ein anderer Benutzer die Lizenz für sich beansprucht!

Daher müssen Sie das Benutzerobjekt aus dem Papierkorb von Azure AD wiederherstellen, anstatt Azure AD Connect zu verwenden. Klingt doch einfach, oder? Richtig, aber beachten Sie die folgenden Einschränkungen:

- Es ist sehr schwierig herauszufinden, was genau wiederhergestellt werden muss. Es gibt kein natives Änderungsprotokoll und keinen Vergleichsbericht, der Ihnen bei der Bestimmung der Azure

AD-Objekte hilft, die geändert oder gelöscht wurden. Wie genau sollen Sie nun herausfinden, was wiederhergestellt werden muss?

- Sie können nur solche Objekte wiederherstellen, die kürzlich gelöscht werden. Der Papierkorb von Azure AD bewahrt gelöschte Objekte nur höchstens 30 Tage lang auf. Wenn der Benutzer vor mehr als 30 Tagen gelöscht wurde, haben Sie Pech gehabt.
- Manche Objekte können überhaupt nicht wiederhergestellt werden. Ein dauerhaft gelöschtes Objekt übergeht den Papierkorb. Daher kann es mit nativen Tools nicht wiederhergestellt werden, unabhängig davon, wie lange das Löschen zurückliegt.
- Eine Massenwiederherstellung ist ohne PowerShell nicht möglich. Ein Angreifer von außen, ein wild gewordenes Skript oder ein böswilliger Angehöriger des Unternehmens kann ganz einfach eine große Zahl von unrichtigen Änderungen oder Löschungen in Ihrem Azure AD veranlassen. Es gibt auch keine native Methode, mit der ohne PowerShell mehrere Benutzer gleichzeitig wiederhergestellt werden können.

Oft wird auch nicht das Objekt selbst gelöscht, sondern der Office 365-Lizenztyp des Objekts oder ein Erweiterungsattribut wird fälschlich geändert oder gelöscht. In derartigen Fällen haben Sie richtiges Pech gehabt. Da Nur-Cloud-Attribute nie im lokalen AD aufgezeichnet werden, können weder Azure AD Connect noch native Tools zu einer Wiederherstellung beitragen.

Und zu guter Letzt gibt es auch keine Möglichkeit, bestimmte Attribute wiederherzustellen, die in einem Benutzerobjekt geändert wurden.

Office 365-Gruppen

Office 365-Gruppen werden von Benutzern oft erstellt, um Personen, mit denen sie zusammenarbeiten möchten und Ressourcen, die von diesen Personen gemeinsam verwendet werden sollen, zusammenzufassen, z. B. ein Postfach und ein Kalender in Exchange Online, Team-Sites in SharePoint Online oder Notizbücher in OneNote.

Wenn eine dieser Nur-Cloud-Gruppen versehentlich gelöscht wird, möchten die betroffenen Benutzer, dass sie bald wiederhergestellt wird. Die Gruppe kann aber über Azure AD Connect nicht wiederhergestellt werden, da sie in Ihrem lokalen AD nie existiert hat. Im Papierkorb von Azure AD werden gelöschte Gruppen 30 Tage lang gespeichert, aber das Wiederherstellen von Office 365-Gruppen ist ein komplizierter Vorgang. Die Gruppen können mit der PowerShell oder dem Admin-Center von Exchange wiederhergestellt werden, aber einzelne Attribute oder Gruppen können nicht wiederhergestellt werden.

Wenn z. B. ein böswilliger Benutzer die Mitgliedschaft aufhebt und die Gruppe löscht, kann die Gruppe nur mit ihren Mitgliedern zum Zeitpunkt des Löschens wiederhergestellt werden. Es ist aber nicht möglich, die Mitgliedschaft mit nativen Mitteln zurückzuerhalten. Sie müssten wissen, welche Benutzer gelöscht wurden, aber beim Bestimmen der geänderten oder gelöschten Azure AD-Objekte kann Ihnen wie gesagt kein Änderungsprotokoll und kein Vergleichsbericht von Azure AD helfen.

Azure AD-Gruppen und Gruppenmitgliedschaft

In Organisationen werden Azure AD-Gruppen auch erstellt, um den Zugriff auf Ressourcen effizient und in Übereinstimmung mit Best Practices zu verwalten. Leider muss eine gelöschte Azure AD-Gruppe oder ihre Mitgliedschaft von Grund auf neu erstellt werden. Gruppen und Gruppenmitgliedschaften in Azure AD werden beim Löschen nicht in den Papierkorb verschoben, daher können sie auch nicht mit nativen Mitteln wiederhergestellt werden.

Azure AD-B2B- und B2C-Konten

Azure AD bietet zwei verschiedene Arten von Benutzerkonten zur Unterstützung von externen Kunden und Partnern an: Business-to-Business-Konten (B2B) und Business-to-Consumer-Konten (B2C). Manche Firmen haben Tausende oder sogar Millionen derartiger Konten. Es ist allerdings vorgesehen, dass B2B- und B2C-Konten keine Microsoft Azure Enterprise-Konten sind. Daher sind sie nicht Teil der Azure AD Connect-Synchronisierung. Diese Konten haben verschiedene Zwecke:

- Manche Organisationen verwenden B2B-KOnten zur Authentifizierung von Benutzern von Partnerorganisationen. Angenommen, die USA-Niederlassung eines multinationalen Konzerns ist zu einer hybriden AD-Umgebung gewechselt, und die kanadische Niederlassung ist noch nicht zu Azure AD übergegangen. Die USA-Niederlassung erstellt Azure-B2B-Konten für die kanadischen Mitarbeiter, damit diese auf die Cloud-Anwendungen und -Dokumente zugreifen können.
- Mit B2C-Konten haben Sie die Möglichkeit, Benutzer Ihrer mobilen und Web-Apps in Ihr Azure AD über eine beliebige im Direktverbund unterstützte Identität einzuladen, z. B. über ein Facebook-, Microsoft- oder Google+-Konto. B2C-Konten sind bereits auf sehr vielen vertikalen Märkten äußerst beliebt, so z. B. im Finanz-, Gesundheits- und Versicherungswesen sowie im Einzelhandel. Ein Unternehmen können seinen Kunden z. B. die Anmeldung bei seinem Azure AD über die LinkedIn-Benutzerinformationen gestatten. Das Unternehmen erstellt ein B2C-Konto für Kunden, das ihnen die Zugriff auf bestimmte Anwendungen und Daten gestattet.

Ein dauerhaft gelöschtes Objekt übergeht den Papierkorb. Daher kann es mit nativen Tools nicht wiederhergestellt werden, unabhängig davon, wie lange das Löschen zurückliegt.

Wenn ein B2B- oder B2C-Konto gelöscht wird, kann sich der Benutzer nicht mehr anmelden und nicht mehr auf die benötigten Ressourcen und Daten zugreifen. Die Gruppe kann über eine lokale Lösung nicht wiederhergestellt werden, da sie in Ihrem lokalen AD nie existiert hat. Stattdessen müssen Sie es mit den oben besprochenen Einschränkungen aus dem Papierkorb von Azure AD wiederherstellen.

Wenn ein B2B- oder B2C-Konto gelöscht wird, kann sich der Benutzer nicht mehr anmelden und nicht mehr auf die benötigten Ressourcen und Daten zugreifen. Die Gruppe kann über eine lokale Lösung nicht wiederhergestellt werden, da sie in Ihrem lokalen AD nie existiert hat. Stattdessen müssen Sie es mit den oben besprochenen Einschränkungen aus dem Papierkorb von Azure AD wiederherstellen.

Andere Nur-Cloud-Benutzerkonten

Neben der Synchronisierung von Benutzerobjekten in einem lokalen AD bei Verwendung von Azure AD Connect erstellen manche Organisationen Azure AD-Konten unter Verwendung eines externen Verzeichnisses, z. B. eines virtuellen Verzeichnisses, oder ihrer Identitätsverwaltung. Es können auch Nur-Cloud-Benutzerobjekte erstellt werden, die die Mitarbeiter bei der Herstellung einer Verbindung mit einer SaaS-Anwendung wie Concur oder Salesforce über Azure AD unterstützt. Die lokale Sicherung und Wiederherstellung erfasst die Benutzerkonten und deren Eigenschaften nicht.

Objekte, die aus Quellen außerhalb des lokalen AD synchronisiert werden

Manche Anwendungen, insbesondere die im eigenen Haus erstellten, arbeiten nicht nativ mit AD zusammen – entweder absichtlich oder aufgrund ihrer Funktion. Sie schreiben außerhalb des nativen Synchronisierungsprozesses direkt auf Azure AD. Beispiele dafür sind Software für die mehrstufige Authentifizierung, die auf Azure AD schreibt, um den Benutzerzugriff zu ermöglichen, und Anwendungen, die Daten in eine erweiterte Azure AD-Umgebung schreiben, um Benutzer zu validieren.

Ohne Synchronisierung von Azure AD werden diese Objekte nicht von der lokalen Sicherung und Wiederherstellung erfasst.

MANDANT-ZU-MANDANT-MIGRATION

Einen anderen selten beachteten Verwendungsfall stellt z. B. die Mandant-zu-Mandant-Migration wegen der Organisations- und Rollenänderungen während einer Konsolidierung, Fusion, Übernahme oder Veräußerung dar. Manche Unternehmen betrachten Azure AD als Teil Ihrer Sicherungs- und Wiederherstellungsstrategie.

Angenommen, ein Unternehmen wird konsolidiert. Es hat Dutzende von Mandanten und muss Benutzer wegen Änderungen der Mitarbeiterrollen und des Berichtswesens zwischen Mandanten verschieben. Es erkennt aber, dass es klug ist, unvorhergesehene Situationen während der Konsolidierung zu berücksichtigen: es könnte z. B. erforderlich sein, für bestimmte Benutzer die alten Anwendungsberechtigungen wiederherzustellen oder bestimmten Benutzern mehrere temporäre Zugriffsstufen zu gewähren. Denken Sie z. B. an ein Unternehmen, bei dem ein ganzer Geschäftszweig aufgelöst und ein Mandant mit Hunderten oder Tausenden von Benutzerkonten ausgegliedert wird. Es wäre klug und umsichtig, eine letzte Sicherung der Konten zu behalten.

Manche Unternehmen verfügen über Dutzende oder sogar über Hunderte von Azure AD-Mandanten für ihre verschiedenen Geschäftseinheiten, die von unterschiedlichen Teams verwaltet werden. Wenn sie sich bei der Migration auf Azure AD als Sicherheitsnetz verlassen und etwas bei der Mandant-zu-Mandat-Migration oder bei der Konsolidierung schief geht, werden sie feststellen, dass native Tools für diese Art von Notfallwiederherstellung wenig geeignet sind.

SICHERUNG UND WIEDERHERSTELLUNG AUF ENTERPRISE-NIVEAU FÜR HYBRIDE UMGEBUNGEN

Es ist aus Sicherheits- und Compliance-Gründen und im Interesse der Geschäftskontinuität entscheidend, über eine zuverlässige Sicherung und Wiederherstellung zu verfügen. Wie wir gesehen haben, ist eine solide lokale Lösung notwendig, aber nicht ausreichend , da es praktisch unmöglich ist, Office 365 oder Azure auszuführen, ohne Nur-Cloud-Benutzer, -Gruppen und -Attribute zu erstellen. Der Papierkorb von Azure AD stellt eine bequeme Möglichkeit dar, bestimmte vor kurzer Zeit gelöschte Objekte wiederherzustellen, aber er war nie als Enterprise-Lösung für die Sicherung und Wiederherstellung gedacht.

Mit Lösungen von Quest können Sie Ihre gesamte hybride Umgebung schützen. Recovery Manager for Active Directory kann nun mit Quest On Demand Recovery integriert werden und bietet so eine vollständige, hybride Wiederherstellungslösung, mit der Sie ruhig schlafen können.

Recovery Manager for AD schützt mehr als 1.600 Organisationen vor unvorhergesehenen oder böswilligen Änderungen ihrer Active Directory-Daten. Es erfasst auch beliebige lokale Objekte, die über Azure AD Connect mit der Cloud synchronisiert wurden, ohne dass Active Directory vom Netz genommen werden muss. Sie können Datensicherungen automatisieren, durch Vergleich der aktuellen Active Directory-Konfiguration mit einer

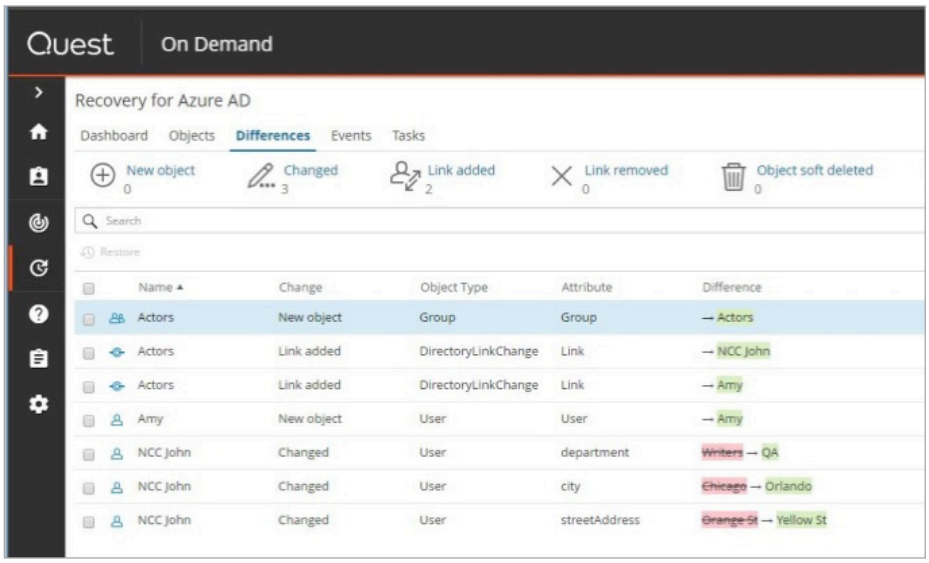

Abbildung 2. Mit Berichten über Unterschiede zwischen Sicherungen und dem Live-Azure AD ist es einfach, Änderungen zu erkennen und genau die gewünschten Änderungen auszuwählen und wiederherzustellen.

Datensicherung Änderungen ermitteln und ganze Abschnitte des gesamten Verzeichnisses, ausgewählte Objekte oder einzelne Attribute wiederherstellen.

Quest On Demand Recovery kümmert sich um den Rest, z. B. um Objekte, die von Azure AD Connect nicht synchronisiert werden.

Durch Verbindung dieser beiden Lösungen erhalten Sie ein einziges Wiederherstellungs-Dashboard sowohl für hybride als auch für Nur-Cloud-Objekte mit von nativen Tools nicht angebotenen Details, z. B. dem Objekttyp. Sie können Differenzberichte ausführen lassen, um festzustellen, was wiederhergestellt werden muss, und jede Änderung direkt aus dem Bericht wiederherstellen, ob im lokalen AD oder im Azure AD (siehe Abbildung 2).

Mit der Quest On-Demand-Wiederherstellung können Sie den Verlauf der Synchronisierung der Objekte mit Azure AD Connect überwachen. Sie können Nur-Cloud-Objekte und -Attribute ermitteln, die nicht synchronisiert werden, und eine unvollständige Wiederherstellung von Objekten vermeiden.

FAZIT

Viele Organisationen verlassen sich zur Synchronisierung eines lokalen AD zu Azure AD auf Azure AD Connect. Diese Art von Einbahnstraßen-Synchronisierung lässt eine Lücke in der Abdeckung der Notfallwiederherstellungs-Strategie, da sich Nur-Cloud- Objekte und -Attribute außerhalb der Reichweite der Tools für die lokale Sicherung und Wiederherstellung befinden.

Nachdem nun der Hybrid-Geist aus der Flasche ist, nutzen die Unternehmen verstärkt Nur-Cloud-Attribute, Office 365-Gruppen, Azure AD-Gruppen, B2B-/B2C-Konten und andere Merkmale einer hybriden AD-Umgebung, um die Benutzerfreundlichkeit zu verbessern. Mit steigender Verwendung wird das Ausfüllen der Lücken in der Notfallwiederherstellungs-Strategie für die Cloud immer dringlicher.

Durch die Integration von Quest Recovery Manager for AD mit Quest On Demand kann ein einziges Wiederherstellungs-Dashboard bereitgestellt werden, das zum Ausfüllen dieser Lücken beiträgt. Unternehmen können mithilfe der Lösung von Quest zwischen hybriden und Nur-Cloud-Objekten unterscheiden, sie können Differenzberichte zwischen Produktion und Echtzeit-Datensicherungen ausführen und Änderungen sowohl lokal als auch in Azure AD wiederherstellen.

Mit der Quest On-Demand-Wiederherstellung können Sie den Verlauf der Synchronisierung der Objekte mit Azure AD Connect überwachen. Sie können Nur-Cloud-Objekte und -Attribute ermitteln, die nicht synchronisiert werden, und eine unvollständige Wiederherstellung von Objekten vermeiden.

ÜBER QUEST

Bei Quest versuchen wir, komplexe Herausforderungen mit einfachen Lösungen zu bewältigen. Dies gelingt uns dank unserer speziellen Unternehmensphilosophie, bei der hervorragender Service und unser allgemeines Ziel – ein unkomplizierter Geschäftspartner zu sein – im Vordergrund stehen. Unsere Vision besteht darin, Technologien bereitzustellen, bei denen Sie sich nicht zwischen Effizienz und Effektivität entscheiden müssen. Dadurch müssen Sie und Ihre Organisation sich weniger um die IT-Verwaltung kümmern und haben mehr Zeit für Unternehmensinnovation.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an:

Quest Software Inc.
Attn: LEGAL Dept

Informationen zu unseren regionalen und internationalen Standorten finden Sie auf unserer Website (www.quest.com/de).