Dell EMC Unity™-Produktreihe Configuring Hosts to Access SMB File Systems

Version 4.5

Part Number: 302-002-566
January 2019
Rev. 04

DELL Technologies

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: HINWEIS enthält wichtige Informationen, mit denen Sie Ihr Produkt besser nutzen können.

VORSICHT: ACHTUNG deutet auf mögliche Schäden an der Hardware oder auf den Verlust von Daten hin und zeigt, wie Sie das Problem vermeiden können.

WARNUNG: WARNUNG weist auf ein potenzielles Risiko für Sachschäden, Verletzungen oder den Tod hin.

Contents

Vorwort

Es werden regelmäßig neue Software- und Hardwareversionen veröffentlicht, um das Produkt kontinuierlich zu verbessern. Aus diesem Grund werden einige in diesem Dokument beschriebene Funktionen eventuell nicht von allen Versionen der von Ihnen verwendeten Software oder Hardware unterstützt. In den Versionshinweisen zum Produkt finden Sie aktuelle Informationen zu Produktfunktionen. Wenden Sie sich an Ihren Experten für technischen Support, wenn ein Produkt nicht ordnungsgemäß oder nicht wie in diesem Dokument beschrieben funktioniert.

Hier erhalten Sie Hilfe

Auf Support, Produkt- und Lizenzierungsinformationen kann wie folgt zugegriffen werden:

Produktinformationen

Dokumentationen oder Versionshinweise zum Produkt und zu Funktionen finden Sie in der Technischen Dokumentaktion von Unity unter dell.com/unitydocs.

Fehlerbehebung:

Informationen über Produkte, Softwareupdates, Lizenzierung und Service finden Sie auf der Supportwebsite (Registrierung erforderlich) unter: dell.com/support. Melden Sie sich an und suchen Sie die entsprechende Produktseite.

1

Einrichten eines Hosts für SMB-Speicher

Dieses Kapitel umfasst folgende Themen:

Themen:

Anforderungen für die Einrichtung eines Hosts

Folgende Anforderungen an das System und das Netzwerk müssen erfüllt sein, bevor Sie einen Host für Unity-Speicher einrichten können.

Bevor Sie einen Host für Unity-Speicher einrichten können, müssen folgende Anforderungen an das Speichersystem und das Netzwerk erfüllt sein.

Übersicht

In diesem Thema werden der Zweck dieses Dokuments und die Zielgruppe beschrieben. Außerdem wird die zugehörige Dokumentation aufgelistet.

Dieses Dokument ist Teil der Unity-Dokumentation. Beschrieben wird das Einrichten von Windows-Hosts mit Clients, die auf Server Message Block (SMB)-Dateisystemspeicher auf einem Unity-System zugreifen müssen.

Dieses Dokument richtet sich an die Person(en), die für die Konfiguration von Hosts für den Zugriff auf Unity-Speicher verantwortlich ist/sind.

Leser dieses Dokuments sollten vertraut sein mit Unity-SMB-Dateisystemspeicher und dem Windows-Betriebssystem auf Hosts mit Clients, die auf Unity-SMB-Dateisystemspeicher zugreifen.

Andere Unity-Dokumente:

- *Installationsanleitung*
- *Hardwareinformationshandbuch*
- *Konfigurieren von Hosts zum Zugriff auf NFS-Dateisysteme*
- *Konfigurieren von Hosts zum Zugriff auf Fibre-Channel-(FC)- oder iSCSI-LUNs*
- *Konfigurieren von Hosts für den Zugriff auf VMware NFS- oder VMware VMFS-Datenspeicher*
- *EMC Storage Integrator für Windows Suite*
- *Unisphere CLI-Benutzerhandbuch*

Die Unisphere-Hilfe bietet spezielle Informationen über Unity-Speicher, -Merkmale und -Funktionen.

Systemanforderungen

Vor dem Konfigurieren von Hosts zum Zugriff auf das Speichersystem stellen Sie sicher, dass diese Anforderungen erfüllt sind.

Führen Sie die folgenden Aufgaben vor dem Verbinden von Hosts mit dem Speichersystem aus:

- Installieren und konfigurieren Sie das System mithilfe des Assistenten für die **Erstkonfiguration**.

- Verwenden Sie Unisphere oder die CLI, um NAS-Server oder -Schnittstellen oder iSCSI- oder Fibre-Channel (FC)-LUNs auf dem Speichersystem zu konfigurieren.

Netzwerkanforderungen

In diesem Thema werden die Netzwerkanforderungen an einen Host aufgeführt, der mit dem Speichersystem verbunden ist.

Stellen Sie sicher, dass Sie diese Netzwerkanforderungen beachten:

- Der Host (Client) muss sich gemeinsam mit dem NAS-Server in einer LAN-Umgebung befinden.
- Der NAS-Server kann entweder ein Mitglied der Windows Active Directory-Domain sein oder unabhängig von einer Windows-Domain als eigenständiger SMB-Server operieren.
- Bei SMB-Shares, die sich in einer Windows Active Directory-Domain befinden, müssen Sie auch DNS und NTP konfigurieren.
- Wenn der NAS-Server für Multiprotokoll (SMB und NFS) aktiviert ist, konfigurieren Sie Unix-Verzeichnisdienste (UDS) mithilfe des Protokolls NIS oder LDAP, lokaler Dateien oder lokaler Dateien und eines UDS.
- In der Unisphere-Onlinehilfe wird beschrieben, wie Sie den Unix-Verzeichnisdienst (entweder NIS oder LDAP) auf der Unity konfigurieren können.

SMB-NAS-Server in einer Windows-Domain

In diesem Thema werden SMB-NAS-Server in einer Windows Active Directory-Domain beschrieben.

Für einen SMB-NAS-Server mit aktiviertem Active Directory gilt Folgendes:

- Verwendet domainbasierte Kerberos-Authentifizierung
- Behält seine eigene Identität (Computerkonto) in der Domain
- Nutzt die Informationen des Domainstandorts, um Services wie z. B. Domaincontroller zu lokalisieren.

Durch Verknüpfung eines SMB-NAS-Servers mit einer Windows-Domain sind alle Benutzer in der Domain mit dem SMB-Server verbunden. Darüber hinaus werden die Authentifizierungs- und Autorisierungseinstellungen des Active Directory-Servers auf die Dateien und Ordner des SMB-Dateisystems angewendet.

Ein SMB-NAS-Server mit aktiviertem Active Directory erfordert eine Windows-Domain mit einem Active Directory (AD)-Server und einem DNS-Server. Sie müssen auch NTP konfigurieren.

Eigenständiger SMB-NAS-Server

In diesem Thema wird ein eigenständiger SMB-NAS-Server beschrieben.

Eigenständige SMB-NAS-Server haben keinen Zugriff auf eine Windows-Domain oder ihre verknüpften Services. Nur Benutzer, deren lokale Benutzerkonten auf dem eigenständigen SMB-NAS-Server erstellt und gemanagt werden, können auf den Server zugreifen. Der SMB-Server führt die Benutzerauthentifizierung durch.

Ein eigenständiger SMB-NAS-Server erfordert eine Windows-Arbeitsgruppe.

Hostsoftware in einer SMB-Umgebung

Dieses Thema bietet einen Überblick über die Hostsoftware für ein Unity-System in einer SMB-Umgebung.

Dieser Abschnitt enthält eine Beschreibung der für Unity-Systeme in SMB-Umgebungen verfügbaren Hostsoftware sowie eine Anleitung zur Installation dieser Software auf einem Host, der Unity-SMB-Dateisystemspeicher verwendet.

Common AntiVirus Agent

Dieses Thema beschreibt die Virenschutzlösung für SMB-Clients mithilfe von Unity-Systemen.

Der Common AntiVirus Agent (CAVA) bietet eine Virenschutzlösung für SMB-Clients, die Unity-Systeme verwenden. VEE CAVA verwendet Virenschutzsoftware von Drittanbietern, um bekannte Viren zu identifizieren und eliminieren, bevor sie Dateien auf dem System infizieren. CAVA ist Teil des CEE-Softwarepakets (Common Event Enabler). Informationen über die Drittanbieter-Virenschutzsoftware, die CAVA unterstützt, finden Sie in der Unity-Supportmatrix auf der Supportwebsite. Informationen

über die Installation des Enablers finden Sie unter *Verwenden des Common Event Enabler auf Windows-Plattformen* auf der Supportwebsite.

Management-Snap-ins

In diesem Thema werden die Management-Snap-ins, die ein Unity-NAS-Server unterstützt, aufgelistet.

Ein NAS-Server unterstützt das Unity NAS-Verwaltungs-Snap-in, das folgende Microsoft Management Console (MMC)-Snap-ins umfasst. Mit diesen Snap-ins können Sie Basisverzeichnisse, Sicherheitseinstellungen und Virusprüfungen auf einem NAS-Server Ordner auf einem Windows-Computer managen:

- Basisverzeichnis-Management-Snap-in
- NAS-Server-Management-Snap-in
- Virenschutzmanagement-Snap-in

Basisverzeichnismanagement-Snap-in

In diesem Thema:a wird beschrieben, wie die Basisverzeichnisfunktion das Management von persönlichen Shares vereinfacht.

Mit dem Basisverzeichnismanagement -Snap-in können Sie einen Benutzernamen mit einem Verzeichnis verknüpfen. Das Verzeichnis ist dann das Basisverzeichnis des Benutzers. Die Basisverzeichnisfunktion vereinfacht das Management von persönlichen Shares und die Verbindung zu ihnen, da Sie den Share-Namen HOME verwenden können, mit dem alle Benutzer verbunden sind.

NAS-Server-Management-Snap-in

In diesem Thema wird die Verwendung der Nodes für Audit-Policies und die Zuweisung von Benutzerrechten des NAS Server-Management-Snap-in beschrieben.

Audit-Policy-Node

Mit dem Überwachungs-Policy-Knoten unter den NAS Server Sicherheitseinstellungen können Sie festlegen, welche Sicherheitsereignisse für NAS-Server im Sicherheitsprotokoll protokolliert werden. Sie können das Sicherheitsprotokoll dann in der Windows-Ereignisanzeige anzeigen. Sie können erfolgreiche Versuche, fehlgeschlagene Versuche, beides oder nichts protokollieren. Die Überwachungsrichtlinien im Audit-Policy-Node sind eine Untergruppe der Richtlinien, die als Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) in Active Domain Users and Computers verfügbar sind. Überwachungsrichtlinien sind lokale Policies und gelten für den ausgewählten NAS-Server. Sie können mit dem Audit-Policy-Node keine GPO-Überwachungsrichtlinien verwalten.

Node für die Zuweisung von Benutzerrechten

Mit dem Node für die Zuweisung von Benutzerrechten können Sie managen, welche Benutzer und Gruppen Anmelde- und Aufgabenrechte für einen NAS-Server haben. Die Benutzerrechtzuweisungen, die im Node für die Zuweisung von Benutzerrechten angezeigt werden, sind eine Untergruppe der Benutzerrechtzuweisungen, die als GPOs in Active Domain Users and Computers verfügbar sind. Benutzerrechtzuweisungen sind lokale Policies und gelten für den ausgewählten NAS-Server. Mit dem Node für die Zuweisung von Benutzerrechten können Sie keine GPO-Richtlinien verwalten.

Allgemeines Virenschutzmanagement-Snap-in

Mit dem allgemeinen Virenschutzmanagement-Snap-in können Sie die Virusprüfungsparameter (viruschecker.conf-Datei) für Common AntiVirus Agent (CAVA) und Virenschutzprogramme von Drittanbietern verwalten.

Installieren der Hostsoftware für SMB

In diesem Thema wird eine Liste der Hostsoftware bereitgestellt, die Sie für die Unity-SMB-Umgebungen installieren können, der Zweck der einzelnen Softwarepakete, die Systeme, auf denen die Pakete installiert werden können, sowie die Installationsschritte.

Info über diese Aufgabe

Tabelle 1. Hostsoftware für Unity-SMB-Umgebungen

Software	Zweck	Installationsort
Basisverzeichnis-Management-Snap-in	Verwalten von Benutzer-Basisverzeichnissen.	Das Windows-System, auf dem Sie die Unity-NAS-Server in der Domain verwalten.
NAS-Server-Management-Snap-in	Überwachen von Sicherheitsereignissen für NAS-Server im Sicherheitsprotokoll und Verwalten des Benutzer- und Gruppenzugriffs und der Aufgabenrechte für einen NAS-Server.	Das Windows-System, auf dem Sie die Unity-NAS-Server in der Domain verwalten.
CEE-Virenschutzmanagement-Snap-in	Verwalten von Virenprüfungsparametern für CAVA und Virenschutzprogrammen von Drittanbietern.	Das Windows-System, das Unity-Speicher verwendet. Erfordert einen oder mehrere Windows-Hosts, bei denen es sich um Antivirenserver (AV) handelt. Bei diesen AV-Servern kann es sich auch um Hosts handeln, die Unity-Speicher verwenden.

So installieren Sie die Hostsoftware für eine SMB-Umgebung auf einem Unity-Host:

Schritte

1. Melden Sie sich beim Host über ein Konto mit Administratorrechten an.
2. Laden Sie das Softwarepaket, das Sie installieren möchten, wie folgt herunter:
   a. Navigieren Sie zum Software-Downloadbereich für die Hostsoftware auf der Online-Support-Website.
   b. Wählen Sie das Softwarepaket, das Sie installieren möchten, und wählen Sie die Option zum Speichern der Software auf dem Host.
3. Doppelklicken Sie in dem Verzeichnis, in dem Sie die Software gespeichert haben, auf die ausführbare Datei, um den Installationsassistenten zu starten.
4. Wählen Sie auf der Seite **Produktinstallation** das Softwarepaket aus, das Sie auf dem Host installieren möchten.
5. Übernehmen Sie den Standardspeicherort für die Programmdateien, indem Sie auf **Weiter** klicken, oder geben Sie einen anderen Speicherort ein, indem Sie den Pfad zum Ordner eingeben oder auf **Ändern** klicken, um zum Ordner zu navigieren. Wenn Sie fertig sind, klicken Sie auf **Weiter**.
6. Klicken Sie auf der Seite **Willkommen** auf **Weiter**.
7. Klicken Sie auf der Seite **Lizenzvereinbarung** auf **Ja.**
8. Prüfen Sie auf der Seite **Installationsordner auswählen**, ob sich der angezeigte Ordnername an dem Speicherort befindet, an dem Sie die Programmdateien installieren möchten, und klicken Sie auf **Weiter**.

   Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**, suchen Sie den Ordner und klicken Sie auf **Weiter**.
9. Wählen Sie auf der Seite **Komponenten auswählen** das Softwarepaket (Komponente) aus, das Sie installieren möchten, deaktivieren Sie die Komponenten, die Sie nicht installieren möchten, und klicken Sie auf **Weiter**.
10. Klicken Sie auf der Seite **Mit dem Kopieren von Dateien beginnen** auf **Weiter**.
11. Klicken Sie auf der Seite **InstallShield Wizard abgeschlossen auf** Fertigstellen.
12. Starten Sie den Host nach Abschluss der Installation neu.

Verwenden der kontinuierlichen Verfügbarkeit von Windows

Seit Windows 8 bieten Windows-Umgebungen die Möglichkeit, Funktionen für die hohe Verfügbarkeit zu SMB-Ressourcen hinzuzufügen. Mit Windows CA können Anwendungen auf Hosts, die mit Shares mit dieser Eigenschaft verbunden sind, ein transparentes Server-Failover für Implementierungen unterstützen, bei denen die Failover-Zeit nicht länger als das Anwendungstimeout ist. In diesen Implementierungen können die Hosts nach einem Failover-Ereignis weiterhin auf eine SMB-Ressource zugreifen, ohne dass ein SMB-Sitzungsstatus verloren geht.

Andere Funktionen wie ein höheres I/O-Volumen, Auslagerungskopien, parallele I/O-Vorgänge während derselben Sitzung sowie Verzeichnisleasing verbessern die Performance und Benutzererfahrung.

Wenn Windows CA auf einer Share aktiviert ist, werden alle I/O-Schreibvorgänge auf die Share als synchrone Write-through-Vorgänge behandelt.

Verwenden von hoher Netzwerkverfügbarkeit

In diesem Thema wird die Verwendung von Linkzusammenfassungen für Konfigurationen mit hoher Verfügbarkeit beschrieben.

Das Unity-System unterstützt Linkzusammenfassungen mit bis zu vier Ethernetports, die mit demselben physischen oder logischen Switch verbunden sind und zu einem einzigen logischen Link verknüpft werden. Um die Linkzusammenfassung auf dem System zu konfigurieren, muss jeder Speicherprozessor (SP) denselben Ethernetporttyp und dieselbe Anzahl an Ethernetports aufweisen, da durch die Linkzusammenfassung im Grunde zwei Linkzusammenfassungen erstellt werden – eine auf jedem SP. Dadurch wird hohe Verfügbarkeit bereitgestellt. Wenn einer der Ports in der Linkzusammenfassung ausfällt, leitet das System den Netzwerkverkehr zu einem anderen Port in der Zusammenfassung um. Wenn Sie jedem SP im System ein Ethernet-I/O-Modul hinzufügen, können Sie eine zusätzliche Linkzusammenfassungsgruppe (LAG) auf dem Portsatz im I/O-Modul erstellen.

Link-Zusammenfassungen

In diesem Thema werden die Vorteile und Funktionen von Linkzusammenfassungen beschrieben.

Linkzusammenfassungen nutzen das Link Aggregation Control Protocol (LACP) nach IEEE 802.3ad-Standard.

ANMERKUNG: Linkzusammenfassung gilt nicht für iSCSI-Schnittstellen.

Eine Linkzusammenfassung wird als ein einziger Ethernetlink angezeigt und bietet folgende Vorteile:

- Hohe Verfügbarkeit von Netzwerkpfaden zu und von dem Unity-System: Wenn ein physischer Port einer Linkzusammenfassung ausfällt, ist für die Konnektivität des Systems weiterhin gesorgt.
- Möglicher Gesamtdurchsatzanstieg: Dies liegt daran, dass mehrere physische Ports mit einem logischen Port verbunden werden und eine Verteilung des Netzwerkverkehrs auf die physischen Ports erfolgt.

Obwohl mit Linkzusammenfassungen eine größere Gesamtbandbreite als mit einem einzigen Port erzielt werden kann, erfolgt die Verbindung zu einem beliebigen Client über nur einen physischen Port und wird daher durch die Bandbreite des Ports beschränkt. Wenn die Verbindung zu einem Port ausfällt, schaltet der Switch den Verkehr automatisch zu den verbleibenden Ports in der Gruppe um. Ist die Verbindung wieder hergestellt, nimmt der Switch automatisch den Betrieb mit dem Port als Teil der Gruppe wieder auf.

Sie können bis zu vier Ports in einer Linkzusammenfassung im Unity-System konfigurieren. Bei der Konfiguration einer Linkzusammenfassung werden eigentlich zwei Linkzusammenfassungen konfiguriert – eine auf jedem SP. Wenn ein Port in einer Zusammenfassung ausfällt, leitet das System den Netzwerkverkehr auf einen anderen Port in der Gruppe um.

Switch-Anforderungen

In diesem Thema werden die Switchanforderungen bei der Verwendung von Linkzusammenfassungen beschrieben.

Wenn die Unity-Ports mit unterschiedlichen Netzwerk-Switchen verbunden sind, sollten alle mit diesen Ports verbundenen Switch-Ports so konfiguriert werden, dass sie sofort vom Blocking- in den Forwarding-Modus umschalten und die Listening- und Learning-Phasen des Spanning-Tree-Protokolls beim Auftreten von Schnittstellen überspringen. Für Cisco-Switche bedeutet dies, dass Sie für jeden Switchport, der mit einem Unity-Port verbunden ist, die Portfast-Funktion aktivieren müssen, um dafür zu sorgen, dass der Switch den Ethernet-Frame, den das Speichersystem bei Aktivierung eines physischen Links erzeugt, weiterleitet. Sie aktivieren die Portfast-Funktion von Port zu Port. Wenn diese Option aktiviert ist, lässt die Portfast-Variable

den Port sofort vom Blocking- in den Forwarding-Modus wechseln. Verwenden Sie die Portfast-Funktion nicht bei Switch-zu-Switch-Verbindungen.

Für die Linkzusammenfassung müssen die Netzwerk-Switches vom IEEE 802.3ad-Protokoll unterstützt werden und sie müssen darauf achten, dass Pakete einer einzelnen TCP-Verbindung immer über denselben Link in eine einzige Richtung versendet werden.

Konfigurieren einer Link-Zusammenfassung

In diesem Thema wird die Konfiguration der Linkzusammenfassung beschrieben. Darüber hinaus werden die erforderlichen Konfigurationsaufgaben aufgeführt.

Für die Linkzusammenfassung ist mindestens ein 802.3ad-konformer Switch erforderlich, wobei jeder Switch über einen verfügbaren Port für jeden Switchport, den Sie mit einem Unity-Port in der Zusammenfassung verbinden möchten, verfügen muss.

Der Begriff NIC-Teaming bezeichnet alle NIC-Redundanz-Schemata, einschließlich Linkzusammenfassung mit 802.3ad.

Für die Linkzusammenfassung müssen Sie zwei Arten von Konfigurationsaufgaben ausführen:

- Konfigurieren einer Linkzusammenfassung vom Switch zum Unity-System
- Konfigurieren einer Linkzusammenfassung vom Host zum Switch

Konfigurieren der Linkzusammenfassung vom Switch zum Unity-System

Erfahren Sie, wie Sie die Switchports konfigurieren und diese in einer Linkzusammenfassung zusammenfassen.

Schritte

1. Konfigurieren Sie die mit dem Unity-System verbundenen Switchports für LACP im aktiven Modus. Details finden Sie in der im Lieferumfang des Switch enthaltenen Dokumentation.
2. Fassen Sie die Ports in einer Linkzusammenfassung mit Unisphere zusammen. Gehen Sie hierfür folgendermaßen vor:
   a. Wählen Sie das Symbol **Einstellungen** und dann **Zugriff** > **Ethernet** aus.
   b. Wählen Sie einen Ethernetport und dann **Linkzusammenfassung** > **Link-Zusammenfassung erstellen** aus.
   c. Wählen Sie die Ports für die Linkzusammenfassung aus und wählen Sie dann **Erstellen** aus.

Ergebnisse

Zwei Linkzusammenfassungen werden mit denselben Ports erstellt – eine Zusammenfassung auf jedem SP.

Konfigurieren der Linkzusammenfassung vom Host zum Switch

In diesem Thema wird die Konfiguration der Linkzusammenfassung vom Host zum Switch beschrieben. Die Schritte beinhalten die Konfiguration von Switchports für die Linkzusammenfassung und NIC-Teaming auf dem Host. Die nachfolgend beschriebenen Schritte sind für einen Netzwerkschnittstellentreiber von Intel.

Schritte

1. Konfigurieren Sie die mit dem Host verbundenen Switchports für die Linkzusammenfassung.
2. Konfigurieren von NIC-Teaming auf einem Host mit Windows Server Version 2008 SP2 bis 2016 oder Windows 8.

   ANMERKUNG: Bei Hosts mit Windows Server 2008 bis 2016 und Windows 8 wird die Linkzusammenfassung als NIC-Teaming bezeichnet. Windows Server 2012 R2, 2016 und Windows 8 erkennen automatisch NIC-Teaming auf Unity und konfigurieren den Host für die Verwendung derselben Schnittstellen wie Unity. Eine manuelle Konfiguration ist nicht erforderlich.

   a. Wählen Sie in der **Systemsteuerung Netzwerk und Internet** > **Netzwerkverbindungen** aus.
   b. **Klicken Sie mit der rechten Maustaste im Dialogfeld „Network Connections“ auf eine für das Teaming gewünschte NIC, und klicken Sie auf** Properties**.**
   c. Klicken Sie auf **Konfigurieren**.
   d. Klicken Sie im Dialogfeld **Eigenschaften.** auf die Registerkarte **Teaming**.
3. Gehen Sie in der Registerkarte **Teaming** wie folgt vor:

a. Wählen Sie **Team this adapter with other adapters**.
b. Klicken Sie auf **New Team**.
Der Assistent **New Team** wird geöffnet.

4. Gehen Sie im Assistenten **New Team** wie folgt vor:
a. Geben Sie den Namen für das Team an und klicken Sie auf **Next**.
b. Wählen Sie die anderen NICs für das Team aus und klicken Sie auf **Next**.
c. Wählen Sie den Teamtyp aus und klicken Sie auf **Next**. Um Informationen zu einem bestimmten Typ zu erhalten, wählen Sie den Typ aus, und lesen Sie die Informationen unter dem Auswahlfeld.
d. Klicken Sie auf **Fertigstellen**.
5. Wenn Sie **Adaptive Load Balancing** als Teamtyp ausgewählt haben und das neue NIC-Team für virtuelle Hyper-V-Maschinen verwenden möchten, deaktivieren Sie **Receive Load Balancing**:
a. Klicken Sie auf die Registerkarte **Advanced**.
b. Wählen Sie unter „Settings“ die Option **Receive Load Balancing** aus.
c. Wählen Sie unter „Values“ die Option **Disabled** aus.
d. Klicken Sie auf **OK**.
Das neue Team wird im Dialogfeld **Network Connections** als „Local Area Network Connection“ angezeigt.
6. So nutzen Sie das neue NIC-Team für virtuelle Maschinen:
a. Wählen Sie im Hyper-V-Manager unter „Virtuelle Maschinen“ die virtuelle Maschine aus.
b. Wählen Sie unter „Actions“ **Virtual Network Manager** aus.
c. Wählen Sie im Virtual Network Manager unter „Virtual Networks“ die Option **VM NIC - Virtual Machine Network** aus.
d. Wählen Sie unter „Connection type“ den Netzwerktyp und das NIC-Team aus.
e. Klicken Sie auf **Anwenden**.
f. Nachdem die Änderungen übernommen wurden, klicken Sie auf **OK**.

Konfigurieren von Windows Server 2012 R2 und Windows Server 2016

Schritte

1. Öffnen Sie die Server-Manager-Konsole.
2. Klicken Sie auf **Lokaler Server** auf der linken Seite und suchen Sie das Eigenschaften-Feld (das oberste Feld auf diesem Bildschirm).
3. Suchen Sie **NIC-Teaming** und klicken Sie auf **Deaktiviert**.
4. Drücken und halten Sie im Bereich für Adapter und Schnittstellen die **STRG**-Taste auf der Tastatur und klicken Sie dann auf die Adapter, die Sie einem Team hinzufügen möchten.
5. Klicken Sie auf **AUFGABEN** oben rechts im Abschnitt für Adapter und Schnittstellen und wählen Sie **Neuem Team hinzufügen** aus.
6. Fügen Sie im NIC-Teaming-Fenster einen Namen für das Team hinzu, das Sie erstellen, und wählen Sie alle Adapter aus, die Sie vielleicht übersehen haben.

ANMERKUNG: Wenn Sie den Server aus der Ferne konfigurieren, kann es sein, dass die Verbindung zum Server nach der Erstellung des Teams unterbrochen wird. Dies passiert, wenn Sie über einen Adapter verbunden sind, der dem Team hinzugefügt wird. Sobald das Team erstellt wurde, erhält ein Teaming-Adapter eine Adresse über DHCP und muss mit einer statischen IP-Adresse neu konfiguriert werden, wenn Sie diesem eine zugewiesen hatten.

Wenn Sie das Fenster „Netzwerkverbindungen“ öffnen, sollte Ihr Teaming-Netzwerkadapter angezeigt werden. Sie können ihn bei Bedarf mit einer IP-Adresse konfigurieren.

Mithilfe von SMB-Verschlüsselung

Windows 8- und Windows Server 2012 SMB3-Umgebungen bieten die Möglichkeit, auf Unity-SMB-Dateisystemen gespeicherte Daten zu verschlüsseln, wenn diese Daten zwischen Unity und dem Windows-Host verschoben werden.

ANMERKUNG: In Unisphere wird diese Art der Verschlüsselung als Protokollverschlüsselung bezeichnet.

SMB-Verschlüsselung auf der Share-Ebene wird für eine bestimmte Share aktiviert und beim Zugriff auf diese Share erzwungen. Informationen über das Konfigurieren einer SMB-Verschlüsselung für eine Share finden Sie in der Unisphere-Onlinehilfe.

Optional kann Verschlüsselung auf Systemebene (hier wird die Verschlüsselung in der Registrierung des NAS-Servers festgelegt) erzwungen werden. Dann ist für jeden Share-Zugriff Verschlüsselung erforderlich. Eine Konfiguration auf Clientebene ist nicht erforderlich.

Konfigurieren von SMB-Dateisystemspeicher

Schritte

1. Verwenden Sie Unisphere oder die Unity-CLI, um Unity-SMB-Dateisystemspeicher für den Host (Client) zu erstellen.
2. Informationen zu diesen Aufgaben erhalten Sie in der Unisphere-Onlinehilfe.

Konfigurieren des Benutzerzugriffs auf die SMB-Share

In dieser Aufgabe wird beschrieben, wie Sie den Benutzerzugriff vom Host auf die SMB-Share konfigurieren. Sie benötigen den Namen oder die IP-Adresse des Unity-NAS-Servers.

Info über diese Aufgabe

Der Benutzerzugriff zur Share wird pro Datei mit Active Directory konfiguriert:

Schritte

1. Melden Sie sich beim Windows-Host mit Active Directory von einem Domainadministratorkonto aus an.
   ANMERKUNG: Der Windows-Host muss Zugriff auf die Domain mit dem NAS-Server für die SMB-Share haben.
2. Öffnen Sie das Fenster „Computerverwaltung“:
   a. Öffnen Sie das Computermanagement-MMC-Snap-in bei allen Windows-Betriebssystemen.
   b. Bei einem Host mit Windows Server Version 2008 SP2 bis 2016 oder Windows 8: Klicken Sie auf **Start** und wählen Sie **Systemsteuerung** > **Verwaltung** > **Computerverwaltung**.
3. Klicken Sie in der Struktur **Computerverwaltung** mit der rechten Maustaste auf **Computerverwaltung (lokal)**.
4. Wählen Sie **Verbindung mit anderem Computer herstellen**.
   Das Dialogfeld **Computer auswählen** wird geöffnet.
5. Geben Sie im Dialogfeld **Computer auswählen** den Namen oder die IP-Adresse des NAS-Servers ein, um die Client-SMB-Shares bereitzustellen.
6. Wählen Sie im Computerverwaltungsbaum **Systemprogramme** > **Dateisysteme** > **Shares** aus.
   Die verfügbaren Shares werden rechts angezeigt. Wenn die Unity-Shares nicht angezeigt werden, achten Sie darauf, dass Sie in der richtigen Domain angemeldet sind.
7. Klicken Sie mit der rechten Maustaste auf die Share, deren Berechtigungen Sie ändern möchten, und wählen Sie **Eigenschaften** aus.
8. Klicken Sie auf die Registerkarte **Share-Berechtigungen**.
9. Wählen Sie den Benutzer oder die Gruppe und die Berechtigungen für den ausgewählten Benutzer oder die ausgewählte Gruppe.
10. Klicken Sie auf **OK**.

Zuordnen einer SMB-Share

Diese Aufgabe enthält eine Anleitung für die Verbindung des Hosts mit der SMB-Share. Außerdem wird beschrieben, wie Sie zum Exportpfad für die Share gelangen.

Info über diese Aufgabe

Sie benötigen den Exportpfad für die Share (`\\NASServer\share`), den Sie in Unisphere ermitteln können, wie unten beschrieben.

Schritte

1. Verwenden Sie auf dem Windows-Host die Windows-Funktion für die Zuordnung des Netzwerklaufwerks, um den Host mit der SMB-Share zu verbinden und optional erneut eine Verbindung zur Share herzustellen, wenn Sie sich beim Host anmelden.
2. Wenn Sie den Exportpfad für die Share benötigen, gehen Sie folgendermaßen vor:
   a. Greifen Sie auf Unisphere zu.
   b. Wählen Sie unter **Speicher** die Optionen **Datei** > **SMB-Shares** aus.
   c. Fügen Sie die Spalte **Exportpfad** zur Ansicht hinzu.
   d. Suchen Sie die SMB-Share auf dem Bildschirm.

   Wenn Sie Lese- und Schreibzugriff auf die Share haben, können Sie nach der Zuordnung der Share Verzeichnisse auf der Share erstellen und Dateien in den Verzeichnissen speichern.

2

Migrieren von SMB-Daten zu einem Unity-Speichersystem

Sie können SMB-Daten zu einem Unity-Speichersystem mit einer manuellen Kopie migrieren. Manuelles Kopieren verhindert den Zugriff auf Daten. ACLs und Berechtigungen innerhalb der Dateistruktur bleiben eventuell nicht erhalten.

Dieses Kapitel umfasst folgende Themen:

Themen:

Migrationsumgebung und -einschränkungen

In diesem Thema werden die Anforderungen und Einschränkungen für die Datenmigration beschrieben.

Sie können Daten zum Unity-System durch manuelles Kopieren oder mithilfe eines anwendungsspezifischen Tools (falls verfügbar) migrieren.

Wenn die SMB-Konfiguration, die Sie migrieren möchten, folgende Merkmale aufweist, wenden Sie sich an Ihren Unity-Serviceanbieter:

- Mehr Shares, als Sie migrieren möchten.
- Berechtigungen, die Sie nicht erneut manuell den Unity-Shares zuweisen möchten.
- Shares, die Sie zwischen Unity-Shares aufteilen möchten.
- Shares, die Sie mit anderen Shares auf derselben Unity-Share kombinieren möchten.

Umgebung für die Datenmigration skizziert die Umgebung für die Datenmigration. Merkmale der Migration mit manueller Kopie listet die Merkmale einer Migration durch manuelles Kopieren auf.

Tabelle 2. Umgebung für die Datenmigration

Komponente	Anforderung
Unity-Speicher	Dateisystem mit Share für die Daten in der Share, die Sie migrieren und für die Sie Datenwachstum zulassen möchten
Host	Host mit Lesezugriff für die Share mit den zu migrierenden Daten und mit Schreibzugriff für die Unity-Share für die migrierten Daten
Freigabe	Share, die Sie komplett zur Unity-Share migrieren

Tabelle 3. Merkmale der Migration mit manueller Kopie

Komponente	Eigenschaft
Berechtigungen	Werden evtl. nicht beibehalten
Ausfallzeit	Die Ausfallzeit ist abhängig vom Zeitaufwand für: • Kopieren der Share-Inhalte zur Unity-Share • Rekonfigurieren der Hosts für Verbindung zur Unity-Share

Für Migrationen mit manueller Kopie und mit einer Anwendung hängt die Ausfallzeit vom Zeitaufwand für folgende Vorgänge ab:

- Kopieren der Share-Inhalte zur Unity-Share
- Rekonfigurieren der Hosts für Verbindung zur Unity-Share

Migrieren von Daten

In diesem Thema werden die Aufgaben für die Migration von Daten auf eine Unity-Share aufgeführt.

Um Daten auf eine Unity-Share zu migrieren, richten Sie den Zugriff auf die Share ein. Migrieren Sie anschließend die Daten.

Einrichten des Zugriffs auf eine Unity-Share für den SMB-Host

In diesem Thema werden die Schritte zur Konfiguration des Benutzerzugriffs auf die neue Share in Active Directory und die Zuordnung der Share aufgeführt.

Info über diese Aufgabe

Auf dem Host, den Sie für die Datenmigration verwenden möchten:

Schritte

1. Konfigurieren Sie den Benutzerzugriff für die neue Share in Active Directory.
   Die einzelnen Schritte werden detailliert unter Konfigurieren des Benutzerzugriffs auf die SMB-Share aufgeführt.
2. Ordnen Sie die neue Share zu.
   Die einzelnen Schritte werden detailliert unter Zuordnen einer SMB-Share aufgeführt.

Migrieren von Daten mit einer manuellen Kopie

Dieses Thema umfasst die Schritte zum manuellen Kopieren von Daten aus jeweils einer Share (anstelle der Verwendung eines anwendungsspezifischen Tools).

Info über diese Aufgabe

Eine manuelle Kopie reduziert die Zeit, während der ein Host auf eine Share, die gerade migriert wird, nicht zugreifen kann.

Schritte

1. Wenn Clients die Share aktiv verwenden, trennen Sie die Verbindung für diese und alle anderen Clients, die auf die migrierten Daten zugreifen können.
2. Verwenden Sie die Methode, die am besten für das Kopieren der Daten vom aktuellen Speicherort zur neuen Unity-Share geeignet ist.
   Diese Methode kann ein einfacher Cut-and-Paste- oder Drag-and-Drop-Vorgang sein. Sorgen Sie dafür, dass die ausgewählte Methode benötigte Metadaten wie Dateiattribute, Zeitstempel und Zugriffsrechte beibehält.
3. Verbinden Sie die Clients nach dem Kopiervorgang wieder mit der neuen Share, die vom Unity-System exportiert wurde, und ordnen Sie dieser Share bei Bedarf ein Laufwerk zu.

3

Management von SMB-Dateisystemspeicher mit Windows-Tools

Dieses Kapitel umfasst folgende Themen:

Themen:

Öffnen der MMC für die Computerverwaltung

In diesem Thema wird beschrieben, wie die Microsoft Management Console (MMC) für die Computerverwaltung für einen bestimmten NAS-Server geöffnet wird.

Schritte

1. Melden Sie sich beim Windows-Host, der Teil des Active Directory ist, von einem Domainadministratorkonto aus an.
   Der Windows-Host muss Zugriff auf die Domain mit dem Unity-NAS-Server haben.
2. Öffnen Sie die Seite „Computerverwaltung“:
   - Öffnen Sie das Computermanagement-MMC-Snap-in bei allen Windows-Betriebssystemen.
   - Bei einem Host mit Windows Server Version 2008 SP2 bis 2016 oder Windows 8: Klicken Sie auf **Start** und wählen Sie **Verwaltung** > **Computerverwaltung**.
3. Klicken Sie mit der rechten Maustaste auf **Computerverwaltung**.
4. Wählen Sie **Verbindung mit anderem Computer herstellen**.
5. Geben Sie den Namen des Unity-NAS-Servers ein und klicken Sie auf **OK**.
   Sie müssen als Administrator mit Administratorrechten angemeldet sein, um MMC-Snap-ins verwenden zu können.

Erstellen von Freigaben und Festlegen von Zugriffskontrolllisten

Es wird empfohlen, Unisphere für die Erstellung von SMB-Shares zu verwenden, wie in der Unisphere-Hilfe beschrieben, und anschließend mithilfe von MMC den Zugriff (ACLs) auf die Shares festzulegen. Als Alternative zu Unisphere können Sie nach der Erstellung eines SMB-Dateisystems im Unity-System mit der MMC Shares in diesem Ordner erstellen.

Zur Erstellung einer Windows-Share mit der MMC müssen Sie:

- die Unity-Share des Stammverzeichnisses des Dateisystems mounten und die darin freizugebenden Verzeichnisse erstellen.
- Ein Unity-Administrator sein

Festlegen von Zugriffskontrolllisten für eine vorhandene Share

In diesem Thema wird beschrieben, wie mithilfe der MMC für die Computerverwaltung Zugriffskontrolllisten für eine vorhandene Share festgelegt werden.

Schritte

1. Öffnen Sie die MMC für die Öffnen der MMC für die ComputerverwaltungComputerverwaltung wie in beschrieben.
2. Wählen Sie in der Konsolenstruktur **Dateisysteme** > **Freigaben**.
   Die aktuell verwendeten Freigaben werden rechts angezeigt.
3. Klicken Sie mit der rechten Maustaste auf die Share, deren Berechtigungen Sie ändern möchten und wählen Sie **Eigenschaften** aus.
4. Klicken Sie auf die Registerkarte **Share-Berechtigungen**.
5. Wählen Sie den Benutzer oder die Gruppe und die Berechtigungen für den ausgewählten Benutzer oder die ausgewählte Gruppe.
6. Klicken Sie auf **OK**.

Erstellen einer Share und Festlegen der Zugriffskontrolllisten

In diesem Thema werden die Schritte zur Erstellung einer Share und zur Festlegung der Zugriffskontrolllisten mithilfe der MMC für die Computerverwaltung.

Schritte

1. Öffnen Sie die MMC für die Öffnen der MMC für die ComputerverwaltungComputerverwaltung wie in beschrieben.
2. Klicken Sie in der Konsolenstruktur auf **Dateisysteme** > **Freigaben**.
   Die aktuell verwendeten Freigaben werden rechts angezeigt.
3. Klicken Sie mit der rechten Maustaste auf **Freigaben**, und wählen Sie im Menü **Neue Dateifreigabe**.
   Der **Ordnerfreigabe-Assistent** wird angezeigt.
4. Geben Sie den Namen des freizugebenden Ordners, den Share-Namen für den Ordner und eine Beschreibung der Share ein. Klicken Sie dann auf **Weiter**.
   Der Assistent fordert Freigabeberechtigungen an.
5. Legen Sie Berechtigungen fest, indem Sie eine der Optionen wählen.
   Mit der Option **Freigabe- und Ordnerberechtigungen anpassen** oder **Berechtigungen anpassen** können Sie einzelnen Gruppen und Benutzern Berechtigungen zuweisen.
6. Klicken Sie auf **Fertigstellen**.

Basisverzeichnisfunktion

Die Basisverzeichnisfunktion vereinfacht die Verwaltung von persönlichen Freigaben und die Verbindung zu ihnen, da Sie einen Benutzernamen mit einem Verzeichnis verknüpfen können, das dann das Basisverzeichnis des Benutzers ist. Das Basisverzeichnis ist einem Benutzerprofil zugeordnet, sodass das Basisverzeichnis bei der Anmeldung automatisch mit einem Netzwerklaufwerk verbunden wird.

Die Basisverzeichnisfunktion wird durch das Basisverzeichnismanagement-Snap-in aktiviert, konfiguriert und verwaltet. Mit dieser Funktion können Sie die integrierte Basisverzeichnis-Share nutzen, indem Sie \HOME oder \%Benutzername% verwenden, wenn Sie das Anmeldeprofil des Benutzers definieren. Sie müssen keine separaten Freigaben für jeden Benutzer erstellen.

Die Home Directory-Funktion ist standardmäßig aktiviert.

Wenn Sie das Anmeldeprofil des Benutzers zuordnen und anzeigen möchten, führen Sie einen der folgenden Schritte aus:

- Verwenden Sie \HOME als die integrierte Share und das integrierte Profil:

```
Z:  \\SMBServer1\HOME
```

- Verwenden Sie \%username% als die integrierte Share und das integrierte Profil:

```
Z:  \\SMBServer1\%username%
```

Einschränkungen für Basisverzeichnisse

Der Freigabename HOME ist für das Basisverzeichnis reserviert. Es gelten folgende Einschränkungen und Voraussetzungen.

- Wenn Sie eine Freigabe namens HOME erstellt haben, können Sie die Basisverzeichnisfunktion nicht aktivieren.
- Wenn Sie die Basisverzeichnisfunktion aktiviert haben, können Sie keine Freigabe namens HOME erstellen.

Ein Basisverzeichnis wird im Windows-Benutzerprofil eines Benutzers mithilfe des Universal Naming Convention (UNC)-Pfades konfiguriert: `\\NAS_server\HOME` oder `\\NAS_server\%username%`, wobei *NAS_server* die IP-Adresse, der Computer oder der NetBIOS-Name des NAS-Servers ist.

HOME ist eine spezielle Freigabe, die für die Basisverzeichnisfunktion reserviert ist. Wenn HOME im Pfad für ein Benutzer-Basisverzeichnis verwendet wird und der Benutzer sich anmeldet, wird das Benutzer-Basisverzeichnis automatisch einem Netzwerklaufwerk zugeordnet. Die Umgebungsvariablen HOMEDRIVE, HOMEPATH und HOMESHARE werden automatisch festgelegt.

Konfigurieren des Benutzerprofils in Active Directory

Gehen Sie folgendermaßen vor, um das Anmeldeprofil des Benutzers in Windows Active Directory zu konfigurieren. Es sind ein Windows-Server und Domain-Administratorkonto erforderlich.

Schritte

1. Melden Sie sich beim Windows-Server von einem Domainadministratorkonto aus an.
2. Wählen Sie in der Systemsteuerung **Verwaltungstools** > **Active Directory-Benutzer und -Computer** aus.
3. Klicken Sie auf **Benutzer**, um im rechten Fenster die Benutzer anzuzeigen.
4. Klicken Sie mit der rechten Maustaste auf einen Benutzer, und wählen Sie **Eigenschaften**.
   Das Fenster **Benutzereigenschaften** für den Benutzer wird angezeigt.
5. Klicken Sie auf die Registerkarte **Profil** und unter Basisordner:
   a. Wählen Sie **Verbinden**.
   b. Wählen Sie das Laufwerk, das Sie dem Basisverzeichnis zuordnen möchten.
   c. Geben Sie bei **Mit** Folgendes ein: **`\\NAS_server\HOME`** oder \\NAS_server\%username%, wobei *NAS_server* die IP-Adresse, der Computer oder der NetBIOS-Name des Unity-NAS-Servers ist.
6. Klicken Sie auf **OK**.

Hinzufügen eines Basisverzeichnisses mit Ausdrücken

In diesem Thema werden die Schritte zum Hinzufügen eines Basisverzeichnisses mit Ausdrücken aufgeführt. Für dieses Verfahren ist ein Domainadministratorkonto erforderlich.

Schritte

1. Melden Sie sich beim Windows-Server von einem Domainadministratorkonto aus an.
2. Wählen Sie in der Systemsteuerung **Verwaltungstools** > **EMC Unity VNX VNXe NAS-Management** aus.
3. Klicken Sie mit der rechten Maustaste auf das Ordnersymbol **Basisverzeichnis** und wählen Sie **Neu** > **Basisverzeichniseintrag** aus.
   Die Seite mit den Basisverzeichniseigenschaften wird angezeigt.
4. Geben Sie die folgenden Informationen ein:
   a. Geben Sie unter **Domain** den Namen der Benutzerdomain ein (NetBIOS-Name).

      ANMERKUNG: Verwenden Sie nicht den vollständig qualifizierten Domainnamen.

      Beispiel: Wenn der Domainname „Company.local“ ist, können Sie Folgendes eingeben: **`company`**, **`comp`** oder **`.*`**. (Reguläre Ausdrücke müssen wahr sein, damit diese Option funktioniert.)
   b. Geben Sie unter **Benutzer** den Namen des Benutzers oder die Platzhalter-Zeichenfolge ein.

      Beispiel: Wenn der Benutzername „Tom“ ist, können Sie Folgendes eingeben: **`T*`** für Benutzernamen, die mit T beginnen, **`*`** für alle Benutzernamen oder **`[r-v].*`** für Benutzernamen, die mit R, S, T, U oder V beginnen. (Reguläre Ausdrücke müssen wahr sein, damit diese Option funktioniert.)
   c. Geben Sie unter Pfad den Pfadnamen ein:

Geben Sie den Pfad des Ordners ein, z. B. `\HomeDirShare\dir1`.

Klicken Sie auf **Durchsuchen**, und wählen Sie den Ordner aus, oder erstellen Sie einen Ordner.

Wenn Sie den Ordner automatisch erstellen möchten, wählen Sie **Verzeichnis automatisch erstellen**.

Beispiele von Verzeichnissen:

- `\HomeDirShare\dir1\User1`
- `\HomeDirShare\<d>\<u>`. Hiermit werden ein Ordner mit dem Domainnamen `d` und ein Verzeichnis mit dem Benutzernamen `u` erstellt.

5. Klicken Sie auf **OK**.

Beispiel

Ausdrucksformate: Beispiele enthält Beispiele von Ausdrucksformaten zum Hinzufügen eines Basisverzeichnisses.

Tabelle 4. Ausdrucksformate: Beispiele

Domain	Benutzer	Pfad	Optionen	Ergebnis
*	*	`\HomeDirShare\`	Keine	Das Basisverzeichnis aller Benutzer ist `\HomeDirShare`.
*	a*	`\HomeDirShare\`	Keine	Das Basisverzeichnis aller Benutzer, deren Benutzername mit einem „a“ beginnt, ist `\HomeDirShare`.
*	*	`\HomeDirShare\<d>\<u>\`	Auto Create Directory = True	Alle Benutzer haben eigene Verzeichnisse. Beispiel: Das Basisverzeichnis von Benutzer „Bob“ mit der Domain „company“ ist `\HomeDirShare\company\Bob`.
comp	[a-d].*	`\HomeDirShare\FolksA-D\<d>\<u>\`	Auto Create Directory = True Regexp=True	Das Basisverzeichnis von Benutzern mit der Domain „company“, deren Benutzername mit a, b, c oder d beginnt, ist `\HomeDirShare\FolksA-D\company\`, wobei „u“ der Benutzername ist.

Verwenden von Gruppenrichtlinienobjekten

In einem Host-Domain-Controller mit Windows Server Version 2008 SP2 bis 2016 können Administratoren eine Gruppenrichtlinie verwenden, um die Konfigurationsoptionen für Gruppen von Benutzern und Computern zu definieren. Mit Windows-GPOs können Elemente wie lokale, Domain- und Netzwerksicherheitseinstellungen gesteuert werden. Die Gruppenrichtlinieneinstellungen sind in GPOs gespeichert, die mit den Sitecontainern, Domaincontainern und Organisationseinheit-Containern (Organizational Unit, OU) in Active Directory verbunden sind. Der Domaincontroller repliziert GPOs auf allen Domaincontrollern in der Domain.

Eine Überwachungs-Policy ist eine Komponente des Unity NAS-Management-Snap-in, das als ein Microsoft Management Console (MMC)-Snap-in in die Managementkonsole auf einem System mit Windows Server Version 2008 SP2 bis 2016 installiert ist.

Mit Überwachungs-Policies können Sie festlegen, welche Sicherheitsereignisse für NAS-Server im Sicherheitsprotokoll erfasst werden. Sie können erfolgreiche Versuche, fehlgeschlagene Versuche, beides oder nichts protokollieren. Überwachte Ereignisse werden im Sicherheitsprotokoll der Windows-Ereignisanzeige angezeigt.

Die Überwachungsrichtlinien im Überwachungsrichtlinienknoten sind eine Untergruppe der Richtlinien, die als GPOs in Active Directory-Benutzer und -Computer (Active Directory Users and Computers, ADUC) verfügbar sind. Diese Überwachungs-Policies sind lokale Policies und gelten nur für den ausgewählten NAS-Server. Sie können mit dem Überwachungsrichtlinienknoten keine GPO-Überwachungsrichtlinien verwalten.

Wenn eine Überwachungsrichtlinie als GPO in ADUC definiert ist, überschreibt die GPO-Einstellung die lokale Einstellung. Wenn der Domainadministrator eine Audit-Policy auf dem Domain Controller ändert, wird diese Änderung vom NAS-Server übernommen. Sie können sie über den Audit-Policy-Node anzeigen. Sie können die lokale Überwachungsrichtlinie ändern, sie ist jedoch erst gültig, wenn das GPO für diese Überwachungsrichtlinie deaktiviert ist. Wenn die Überwachung deaktiviert ist, bleibt die GPO-Einstellung in der Einstellungsspalte „Gültig“.

GPO-Unterstützung auf einem -NAS-Server

Ein NAS-Server unterstützt GPOs, indem eine Kopie der GPO-Einstellungen für jeden NAS-Server abgerufen und gespeichert wird, der mit einer Windows Server-Domain verknüpft ist. Ein -NAS-Server speichert die GPO-Einstellungen in seinem GPO-Cache.

Wenn das System hochgefahren wird, liest es die Einstellungen im GPO-Cache und ruft dann die aktuellen GPO-Einstellungen vom Windows-Domaincontroller ab. Nach dem Abruf der GPO-Einstellungen aktualisiert ein -NAS-Server automatisch die Einstellungen basierend auf dem Domain-Aktualisierungsintervall.

Unterstützte GPO-Einstellungen

Ein -NAS-Server unterstützt momentan folgende GPO-Sicherheitseinstellungen:

Kerberos

- Max. Toleranz für die Synchronisation des Computertakts (Uhrabweichung). Die Zeitsynchronisierung erfolgt über den NAS-Server.
- Max. Gültigkeitsdauer des Benutzertickets

Überwachungsrichtlinie

- Anmeldeversuche überwachen
- Kontenverwaltung überwachen
- Verzeichnisdienstzugriff überwachen
- Anmeldeereignisse überwachen
- Objektzugriffsversuche überwachen
- Richtlinienänderungen überwachen
- Rechteverwendung überwachen
- Prozessverfolgung überwachen
- Systemereignisse überwachen

Unter Überwachen von SMB-Benutzern und -Objekten finden Sie weitere Informationen.

Benutzerrechte

- Auf diesen Computer vom Netzwerk aus zugreifen
- Sichern von Dateien und Verzeichnissen
- Auslassen der durchsuchenden Überprüfung
- Zugriff vom Netzwerk auf diesen Computer verweigern
- Virenprüfung
- Generieren von Sicherheitsüberwachungen
- Verwalten von Überwachungs- und Sicherheitsprotokollen
- Wiederherstellen von Dateien und Verzeichnissen
- Übernehmen der Eigentümerschaft von Dateien und Objekten

Sicherheitsoptionen

- Clientkommunikation digital signieren (immer)
- Clientkommunikation digital signieren (wenn möglich)
- Serverkommunikation digital signieren (immer)
- Serverkommunikation digital signieren (wenn möglich)
- LAN Manager-Authentifizierungsebene

Ereignisprotokolle

- Maximale Größe des Anwendungsprotokolls
- Maximale Größe des Sicherheitsprotokolls
- Maximale Größe des Systemprotokolls
- Gastzugriff zum Anwendungsprotokoll einschränken
- Gastzugriff zum Sicherheitsprotokoll einschränken
- Gastzugriff zum Systemprotokoll einschränken
- Anwendungsprotokoll-Aufbewahrung
- Sicherheitsprotokoll-Aufbewahrung
- Systemprotokoll-Aufbewahrung
- Aufbewahrungsmethode des Anwendungsprotokolls
- Aufbewahrungsmethode des Sicherheitsprotokolls
- Aufbewahrungsmethode des Systemprotokolls

Gruppen-Policy

- Hintergrundaktualisierung der Gruppenrichtlinie deaktivieren
- Gruppenrichtlinien-Aktualisierungsintervall für Computer

SMB-Signaturen

SMB-Signaturen sorgen dafür, dass ein Paket nicht abgefangen, geändert oder erneut ausgeführt wird. Es wird sichergestellt, dass das Paket nicht durch einen Drittanbieter geändert wurde. Beim Signieren wird zu jedem Paket eine Signatur hinzugefügt. Der Client und die Unity-NAS-Server verwenden diese Signatur, um die Integrität des Pakets zu prüfen. Die Unity-NAS-Server unterstützen SMB1, SMB2 und SMB3.

Für den Client und den Server einer Transaktion müssen SMB-Signaturen aktiviert sein. SMB-Signaturen sind auf den Unity-NAS-Servern immer aktiviert, jedoch nicht erforderlich. Wenn SMB-Signaturen auf dem Client aktiviert sind, werden Signaturen verwendet. Wenn SMB-Signaturen auf dem Client deaktiviert sind, werden keine Signaturen verwendet. Signierung kann durch Active Directory-Domain-Policy durchgesetzt werden.

Monitoring von Verbindungen von NAS-Servern und der Ressourcennutzung

Mit Windows-Verwaltungsprogrammen können Sie Benutzer, Share-Zugriff und Dateiverwendung auf NAS-Servern überwachen.

Überwachen von Benutzern auf einem NAS-Server

In diesem Thema werden die Schritte zum Monitoring der Anzahl der Benutzer, die eine Verbindung zu einem NAS-Server herstellen, aufgeführt.

Schritte

1. Öffnen Sie die MMC für die Öffnen der MMC für die ComputerverwaltungComputerverwaltung für den NAS-Server, den Sie überwachen möchten (siehe).
2. Klicken Sie in der Konsolenstruktur auf **Freigegebene Ordner** > **Sitzungen**.

   Die aktuell mit dem NAS-Server verbundenen Benutzer werden rechts angezeigt.
3. Optional:
   - Um Verbindungsunterbrechungen vom NAS-Server zu erzwingen, klicken Sie mit der rechten Maustaste auf den Benutzernamen, und wählen Sie im Menü **Sitzung schließen**.
   - Um Verbindungsunterbrechungen für alle Benutzer zu erzwingen, klicken Sie mit der rechten Maustaste auf **Sitzungen**, und wählen Sie im Menü **Alle Sitzungen trennen**.

Überwachung des Zugriffs auf Freigaben auf dem NAS-Server

In diesem Thema werden die Schritte zum Monitoring des Zugriffs auf Shares auf einem NAS-Server aufgeführt.

Schritte

1. Öffnen Sie die MMC für die Computerverwaltung für den NAS-Server (siehe Öffnen der MMC für die Computerverwaltung).
2. Klicken Sie in der Konsolenstruktur auf **Freigegebene Ordner** > **Sitzungen**.
   Die aktuell mit dem NAS-Server verbundenen Benutzer werden rechts angezeigt.
3. Um Verbindungsunterbrechungen von einer Freigabe zu erzwingen, klicken Sie optional mit der rechten Maustaste auf den Freigabenamen, und wählen Sie im Menü **Freigabe beenden**.

Monitoring der Dateiverwendung auf dem NAS-Server

In diesem Thema werden die Schritte zum Monitoring, der Dateiverwendung auf einem NAS-Server mithilfe der MMC für die Computerverwaltung aufgeführt.

Schritte

1. Öffnen Sie die MMC für die Öffnen der MMC für die ComputerverwaltungComputerverwaltung für den NAS-Server (siehe).
2. Klicken Sie in der Konsolenstruktur auf **Dateisysteme** > **Open Files**.
   Die verwendeten Dateien werden rechts angezeigt.
3. Um eine geöffnete Datei zu schließen, klicken Sie optional mit der rechten Maustaste auf die Datei, und wählen Sie im Menü **Geöffnete Datei schließen**.
4. Um alle geöffneten Dateien zu schließen, klicken Sie mit der rechten Maustaste auf den Ordner **Geöffnete Dateien**, und wählen Sie im Menü **Alle geöffneten Dateien trennen**.

Überwachen von SMB-Benutzern und -Objekten

Um NAS-Server zu überwachen, verwenden Sie das Unity NAS-Management-Snap-in (hierbei handelt es sich um ein MMC-Snap-in). Installieren der Hostsoftware für SMB bietet Informationen zur Installation der MMC-Snap-ins.

Standardmäßig ist die Überwachung für alle Windows-Objektklassen deaktiviert. Um die Überwachung zu aktivieren, müssen Sie sie explizit für spezielle Ereignisse auf einem bestimmten NAS-Server aktivieren. Nach der Aktivierung wird die Überwachung auf dem relevanten NAS-Server initiiert. Die Onlinehilfe des Unity NAS-Management-Snap-ins bietet Informationen zur Festlegung der Überwachungsrichtlinien.

Wenn das GPO auf dem NAS-Server konfiguriert und aktiviert ist, wird die GPO-Konfiguration der Überwachungseinstellungen verwendet.

Überwachung ist nur für bestimmte Objektklassen und Ereignisse verfügbar, die in Überwachen von Objektklassen aufgelistet sind. Nur ein Unity Advanced Administrator kann die Überwachung auf einem NAS-Server festlegen.

Tabelle 5. Überwachen von Objektklassen

Objektklasse	Ereignis	Überwacht auf
Anmeldung/Abmeldung	SMB-Benutzername SMB-Gast-Anmeldung	Erfolg
	Domaincontroller gibt Passwort-Authentifizierungsfehler zurück Domaincontroller gibt nicht verarbeiteten Fehlercode zurück Keine Antwort vom DC (unzureichende Ressourcen oder mangelhaftes Protokoll)	Fehler
Datei- und Objektzugriff	Verhalten beim Öffnen eines Objekts:	Erfolg

Tabelle 5. Überwachen von Objektklassen (fortgesetzt)

Objektklasse	Ereignis	Überwacht auf
	• Datei- und Verzeichniszugriff; wenn Systemzugriff-Steuerungsliste (System Access Control List, SACL) festgelegt, Lese-, Schreib-, Lösch-, Ausführungs- und Festlegungsrechte übernehmen • Änderung der lokalen Security Access Manager (SAM)-Gruppe Verhalten beim Schließen: • Datei- und Verzeichniszugriff; wenn SACL festgelegt, Lese-, Schreib-, Lösch-, Ausführungs- und Festlegungsrechte übernehmen • SAM-Datenbank geschlossen Objekt zum Löschen geöffnet: Datei- und Verzeichniszugriff (wenn SACL festgelegt) Objekt löschen: Datei- und Verzeichniszugriff (wenn SACL festgelegt)	
	SAM-Datenbankzugriff (Suche)	Erfolg und Fehler
Prozessverfolgung	Nicht unterstützt	-
Neustarten/Herunterfahren des Systems	Neustarten: • Starten des SMB-Service • Beenden des SMB-Service • Überwachungsprotokoll bereinigt	Erfolg
Sicherheitsrichtlinien	Sitzungsrechte: • Benutzerrechte auflisten • Benutzerrechte zugewiesen • Benutzerrechte gelöscht Richtlinienänderung: Richtlinienkategorien und verknüpften Überwachungsstatus auflisten	Erfolg
Verwendung der Benutzerrechte	Nicht unterstützt	-
Benutzer- und Gruppenverwaltung	Lokale Gruppe erstellen Lokale Gruppe löschen Mitglied zu lokaler Gruppe hinzufügen Mitglied aus lokaler Gruppe entfernen	Erfolg

Wenn die Überwachung aktiviert ist, erstellt die Ereignisanzeige ein Sicherheitsprotokoll mit den Standardeinstellungen (siehe Standardprotokolleinstellungen).

Tabelle 6. Standardprotokolleinstellungen

Protokolltyp	Maximale Dateigröße	Aufbewahrung
Sicherheit	512 KB	10 Tage

Der Unity-NAS-Server unterstützt die Überwachung für einzelne Ordner und Dateien.

Aktivierung der Überwachung auf einem NAS-Server

Führen Sie folgende Schritte durch, um die Überwachung auf einem NAS-Server zu aktivieren:

- Angeben der Audit-Policy
- Festlegen der Überwachungsprotokollparameter

Angeben der Audit-Policy

In diesem Thema werden die Schritte für den Zugriff auf das Sicherheitsverwaltungs-Snap-in und die Angabe der Audit-Policies aufgeführt.

Info über diese Aufgabe

Gehen Sie nach der Installation der Unity-NAS-Management-Konsole wie folgt vor:

Schritte

1. Öffnen Sie die MMC für die Computerverwaltung für den NAS-Server (siehe Öffnen der MMC für die Computerverwaltung).
2. Klicken Sie auf **Start** und wählen Sie **Programme oder Alle Programme** > **Verwaltung** > **Unity NAS-Management** aus.
3. Gehen Sie im Fenster **Unity-NAS-Management** wie folgt vor:
   - Wenn ein NAS-Server ausgewählt ist (ein Name wird hinter Unity-NAS-Management angezeigt), fahren Sie mit Schritt 4 fort.
   - Falls kein NAS-Server ausgewählt ist:
     a. Klicken Sie mit der rechten Maustaste auf **NAS-Server-Management** und wählen Sie **Mit NAS-Server verbinden** aus dem Menü aus.
     b. Wählen Sie im Dialogfeld **NAS-Server auswählen** wie folgt einen NAS-Server aus:
        - Wählen Sie in der Liste **Suchen in** die Domain aus, in der sich der zu verwaltende NAS-Server befindet, und wählen Sie den NAS-Server aus der Liste aus.
        - Geben Sie im Feld **Name** den Netzwerknamen oder die IP-Adresse des NAS-Servers ein.
4. Doppelklicken Sie auf **NAS-Server-Management** und doppelklicken Sie auf **NAS-Server-Sicherheitseinstellungen**.
5. Wählen Sie **Überwachungsrichtlinie**.
   Die Überwachungsrichtlinien werden im rechten Fenster angezeigt.
6. Klicken Sie mit der rechten Maustaste auf **Überwachungsrichtlinie** und wählen Sie im Menü **Überwachung aktivieren**.
7. Doppelklicken Sie im rechten Fenster auf ein Überwachungsobjekt, um die Überwachungsrichtlinie für dieses Objekt zu definieren.
   Die Onlinehilfe des NAS-Management-Snap-in bietet Informationen zur Überwachungsrichtlinie.

Festlegen der Überwachungsprotokollparameter

In diesem Thema werden die Schritte zur Festlegung der Auditprotokollparameter mithilfe der MMC für die Computerverwaltung für den NAS-Server aufgeführt.

Schritte

1. Öffnen Sie die MMC für die Computerverwaltung für den NAS-Server (siehe Öffnen der MMC für die Computerverwaltung).
2. Doppelklicken Sie auf **Event Viewer** und wählen Sie in Windows Server Versionen 2008 SP2 bis 2016 **Windows-Protokolle** aus.
   Die Protokolldateien werden angezeigt.
3. Klicken Sie mit der rechten Maustaste auf die Protokolldatei, und wählen Sie im Menü **Eigenschaften**.
   Das Eigenschaftenblatt für das Protokoll wird angezeigt. In der Regel ist das Feld **Maximale Protokollgröße** gesperrt.
4. Kehren Sie anschließend zum Dialogfeld mit den **Anwendungseigenschaften** für das Protokoll zurück, und klicken Sie auf die Pfeile, um die Größe des Protokolls zu ändern.
5. Geben Sie im Bereich **Protokollgröße** des Dialogfelds an, was geschieht, wenn die maximale Protokollgröße erreicht ist:
   - **Ereignisse bei Bedarf überschreiben**: Gibt an, ob alle neuen Ereignisse in das Protokoll geschrieben werden, selbst wenn das Protokoll voll ist. Wenn das Protokoll voll ist, ersetzt jedes neue Ereignis das älteste Ereignis.
   - **Ereignisse überschreiben, die älter als (*n*) Tage sind:** Überschreibt Ereignisse, die älter als die angegebene Anzahl von Tagen sind. Geben Sie mit den Pfeilen den Grenzwert an, oder klicken Sie auf das Feld, um den Grenzwert

einzugeben. Die in Schritt 4 angegebene Größe der Protokolldatei wird nicht überschritten. Wenn die maximale Protokollgröße erreicht ist und keine älteren Ereignisse vorliegen, werden keine neuen Ereignisse hinzugefügt.

- **Ereignisse nicht überschreiben**: Füllt das Protokoll bis zum in Schritt 4 angegebenen Grenzwert. Wenn das Protokoll voll ist, werden keine neuen Ereignisse hinzugefügt, bis Sie das Protokoll bereinigen.

6. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Anzeigen von Auditereignissen

In diesem Thema werden die Schritte zur Anzeige von Auditereignissen aufgeführt.

Schritte

1. Klicken Sie auf **Start** und wählen Sie **Alle Programme** > **Verwaltung** > **Event Viewer** aus.
2. Klicken Sie mit der rechten Maustaste im rechten Fenster auf das Symbol **Ereignisanzeige**, und wählen Sie im Menü **Verbindung mit anderem Computer herstellen**.
   Das Dialogfeld **Computer auswählen** wird angezeigt.
3. Geben Sie direkt im Dialogfeld **Computer auswählen** den Namen oder die IP-Adresse des NAS-Servers ein. Sie können auch **Durchsuchen** auswählen, um den NAS-Server zu suchen.
4. Klicken Sie in einer Windows Server-Version 2008 SP2 bis 2016 auf **Windows-Protokolle**.
5. Klicken Sie auf das Protokoll.
   Die Protokolleinträge werden im rechten Fenster angezeigt.
6. Doppelklicken Sie auf den Protokolleintrag, um die Ereignisdetails anzuzeigen.
   Das Fenster **Ereigniseigenschaften** wird geöffnet.

Deaktivieren des Auditing

In diesem Thema werden die Schritte zur Deaktivierung des Auditing aufgeführt.

Schritte

1. Melden Sie sich bei einem Domaincontroller mit Windows Server Version 2008 SP2 bis 2016 mit Domain-Administratorrechten an.
2. Klicken Sie auf **Start** und wählen Sie **Programme oder Alle Programme** > **Verwaltung** > **Unity NAS-Management** aus.
3. Führen Sie einen der folgenden Schritte aus:
   - Wenn der NAS-Server bereits ausgewählt ist (Name wird hinter NAS-Server-Management angezeigt), fahren Sie mit Schritt 4 fort.
   - Falls kein NAS-Server ausgewählt ist:
     a. Klicken Sie mit der rechten Maustaste auf **NAS-Server-Management** und wählen Sie **Mit NAS-Server verbinden** aus dem Menü aus.
     b. Wählen Sie im Dialogfeld **NAS-Server auswählen** wie folgt einen NAS-Server aus:
        - Wählen Sie in der Liste **Suchen in** die Domain aus, in der sich der zu verwaltende NAS-Server befindet, und wählen Sie den NAS-Server aus der Liste aus.
        - Geben Sie im Feld **Name** den Netzwerknamen oder die IP-Adresse des NAS-Servers ein.
4. Doppelklicken Sie auf **NAS-Server-Management** und doppelklicken Sie auf **NAS-Server-Sicherheitseinstellungen**.
5. Klicken Sie mit der rechten Maustaste auf **Überwachungsrichtlinie**, und wählen Sie im Menü **Überwachung deaktivieren**.

Zugreifen auf das Sicherheitsprotokoll für einen NAS-Server

Standardmäßig speichert jeder NAS-Server sein Windows-Sicherheitsprotokoll unter `c:\security.evt` (maximale Größe: 512 KB). Sie können über die `C$`-Freigabe jedes NAS-Servers direkt auf dieses Sicherheitsprotokoll zugreifen:

`\\`*`storage_server_netbios_name`*`\C$\security.evt`

wobei *storage_server_netbios_name* der NetBIOS-Name des NAS-Servers ist.

Kopieren eines Share-Snapshot

In diesem Thema werden die Schritte zum Kopieren eines Share-Snapshots mit Windows Explorer aufgeführt.

Schritte

1. Greifen Sie auf den NAS-Server mit der Share, die Sie kopieren möchten, wie folgt zu:
   - Navigieren Sie in Windows Explorer zum NAS-Server.
   - Wählen Sie **Start** > **Ausführen** > ***NAS_server_name*** aus.
2. Klicken Sie auf dem NAS-Server mit der rechten Maustaste auf die Freigabe mit dem Snapshot, den Sie kopieren möchten, und wählen Sie **Eigenschaften** aus.
3. Klicken Sie auf die Registerkarte **Vorherige Versionen**.
4. Wählen Sie den Snapshot (die vorherige Version) aus, den Sie kopieren möchten, und klicken Sie auf **Kopieren**.
   Eine beschreibbare Kopie des Snapshot wird an dem angegebenen Speicherort erstellt.

Wiederherstellen eines Share-Snapshot

In diesem Thema werden die Schritte zur Wiederherstellung eines Share-Snapshot aufgeführt.

Info über diese Aufgabe

Bei der Wiederherstellung einer Speicherressource anhand eines Snapshot wird der vorherige vom Snapshot erfasste Status der Speicherressource wiederhergestellt (Rollback). Dabei wird die gesamte Speicherressource, einschließlich aller Dateien und Daten, durch die Inhalte des Snapshot ersetzt.

ANMERKUNG: Sorgen Sie dafür, dass alle Clients die Lese- und Schreibvorgänge für die Speicherressource abgeschlossen haben, die Sie wiederherstellen möchten, um Datenverlust zu vermeiden.

Schritte

1. Greifen Sie auf den NAS-Server mit der Share, die Sie kopieren möchten, wie folgt zu:
   - Navigieren Sie in Windows Explorer zum NAS-Server.
   - Wählen Sie **Start** > **Ausführen** > ***NAS_server_name*** aus.
2. Klicken Sie auf dem NAS-Server mit der rechten Maustaste auf die Freigabe mit dem Snapshot, den Sie kopieren möchten, und wählen Sie **Eigenschaften.**
3. Klicken Sie auf die Registerkarte **Vorherige Versionen**.
4. Wählen Sie den Snapshot (vorherige Version), den Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellen**.

Ergebnisse

Beim Wiederherstellen geschieht Folgendes:

- Für Dateien in der aktuellen Version on (nicht in der wiederherzustellenden vorherigen Version): Keine Änderung dieser Dateien in der Freigabe.
- Für Dateien in der vorherigen wiederherzustellenden Version und der aktuellen Version: Dateien in der Freigabe werden mit den Inhalten der Dateien der vorherigen Version überschrieben.
- Für Dateien in der wiederherzustellenden vorherigen Version (nicht in der aktuellen Version): Dateien werden zu der Freigabe hinzugefügt.

Beispiel

Beispiel:

- Die aktuelle Version umfasst die Dateien a, b und f.
- Die vorherige Version, die wiederhergestellt wird, umfasst die Dateien a, f und g.

Die wiederhergestellte Version umfasst Datei b mit den Inhalten der aktuellen Version und die Dateien a, f und g mit den Inhalten der vorherigen Version.

4

Verwenden von CEE CAVA mit Unity

Dieses Kapitel umfasst folgende Themen:

Themen:

Überblick über CAVA

Das CEE-Paket (Common Event Enabler) bietet eine Virenschutzlösung (Common Anti-Virus Agent) für Clients, die das Unity-System nutzen. Er nutzt branchenübliche SMB-Protokolle in einem Windows-System. Common Anti-Virus Agent (CAVA) verwendet Virenschutzsoftware eines Drittanbieters, um bekannte Viren zu identifizieren und zu eliminieren, bevor sie Dateien im Unity-System infizieren. Obwohl die Unity-NAS-Server gegen Viren resistent sind, benötigen auch Windows-Clients Schutz. Der Virenschutz auf dem Client reduziert das Risiko, dass der Client eine infizierte Datei auf dem Speicherserver speichert, und schützt den Client, wenn er eine infizierte Datei öffnet.

Die CEE-Lösung umfasst die folgenden Komponenten:

- NAS-Server, auf dem der Client für die CEE CAVA-Virenprüfung ausgeführt wird
- Virenschutz-Engine eines Drittanbieters
- CEE CAVA-Software

Die Virenschutz-Engine eines Drittanbieters und die CEE CAVA-Software müssen auf mindestens einem System mit Windows Server Version 2008 SP2 bis 2016 oder einer Windows 8-Workstation in der Domain mit dem Unity-System installiert sein. Dieser Server wird als Virenschutzserver bezeichnet.

Dieses Kapitel beschreibt, wie Sie CEE CAVA mit Unity verwenden. Ausführliche Informationen zum Verwalten von CAVA finden Sie unter *Verwenden des Common Event Enabler auf Windows-Plattformen* auf der Supportwebsite.

Unity-NAS-Server

Auf den Unity-NAS-Servern wird der Betrieb für Windows-Dateisysteme und -Shares (SMB) und/oder Linux-/UNIX-Dateisysteme und -Shares (NFS) gemanagt. Für eine CEE CAVA-Lösung benötigt das Unity-System mindestens einen NAS-Server, der für SMB konfiguriert ist, sowie Windows-Benutzerzugriff auf Shares.

CEE CAVA-Virenprüfclient

Der Virenprüfclient ist ein CEE CAVA-Agent, der auf dem Unity-NAS-Server ausgeführt wird. Der Virenprüfclient interagiert mit der Virenschutz-Engine, die Anfragen vom Virenprüfclient verarbeitet. Virenschutz wird nur für den SMB-Zugriff unterstützt. Während der Virenprüfung oder anderen verknüpften Aktionen wird der Zugriff auf die Datei von SMB-Clients blockiert.

Der Virenprüfclient:

- stellt die Namen der Dateien in Warteschlangen und gibt diese zur Prüfung an CEE CAVA weiter.
- stellt Ereignisauslöser für Prüfungen bereit und bestätigt sie. Zu den möglichen Ereignisauslösern zählen:
  - Eine Datei wird im Unity-System umbenannt.
  - Eine Datei wird in das Unity-System kopiert oder dort gespeichert.
  - Eine Datei wird im Unity-System geändert und geschlossen.

Unterstützung für Virenschutzsoftware von Drittanbietern

Die CEE CAVA-Lösung nutzt Virenschutzsoftware von Drittanbietern, die sogenannte Virenschutz-Engine, um bekannte Viren zu identifizieren und zu eliminieren, bevor sie Dateien im Unity-System infizieren. Die Virenschutz-Engines, die CAVA unterstützt, finden Sie in der Unity Supportmatrix auf der Supportwebsite.

CEE CAVA-Software

Die CEE CAVA-Software ist eine Anwendung, die auf einem Windows-Server (Virenschutzserver) ausgeführt wird. Sie kommuniziert mit einer Standardvirenschutz-Engine, die auf einem oder mehreren Servern ausgeführt wird, um SMB-Dateien in einem Unity-System zu prüfen.

EMC Unity/VNX/VNXe-NAS-Management-Snap-in

Das EMC Unity/VNX/VNXe-NAS-Management-Snap-in ist ein MMC-Snap-in für Unisphere. Mit diesem Snap-in können Sie die CEE-Virenprüfparameter für die Unity-NAS-Server anzeigen oder ändern.

Systemanforderungen und Einschränkungen

Für die CEE CAVA-Lösung ist Folgendes erforderlich:

- Ein Unity-System mit mindestens einem im Netzwerk konfigurierten NAS-Server.
- Jeder NAS-Server muss über einen CAVA-Pool mit mindestens zwei CAVA-Servern verfügen. Dies wird in der Datei `viruschecker.conf` des NAS-Servers angegeben.
- Installation des Management-Snap-ins in EMC Unity/VNX/VNXe NAS auf einem Clientsystem, das Zugriff auf die Unity-Domain hat. Informationen zur Installation dieses Snap-in finden Sie unter Installieren der Hostsoftware für SMB.
- Unter Windows Server 2008 müssen Sie bei Verwendung des CAVA-Dimensionierungstools Cavamon die Datei `cava.mof` manuell kompilieren.
- Virenschutzsoftware eines Drittanbieters auf einem oder mehreren Virenschutzservern in der Domain. CEE CAVA unterstützt 32-Bit- und 64-Bit-Windows-Umgebungen und entsprechende Virenschutz-Engines von Drittanbietern. Die erforderliche Version der Virenschutz-Engine hängt vom Betriebssystem ab. Die aktuellen Systemanforderungen für Software von Drittanbietern finden Sie auf der entsprechenden Drittanbieter-Website oder in der Drittanbieter-Dokumentation.
- CEE CAVA-Software auf jedem Virenschutzserver in der Domain.

  ANMERKUNG: Mit Ausnahme von Trend Micro muss das Drittanbieter-Virenschutzprogramm vor CEE CAVA auf jedem Virenschutzserver installiert werden. Trend Micro muss nach CEE CAVA installiert werden.

Wir empfehlen dringend, dass der Virenschutzadministrator die Virendefinitionsdateien auf allen lokalen Virenschutz-Engines in den CEE CAVA-Speicherpools aktualisiert.

Nicht-SMB-Protokolle

Die CEE CAVA-Lösung ist nur für Clients gedacht, die das SMB-Protokoll ausführen. Wenn Clients NFS- oder FTP-Protokolle verwenden, um Dateien zu verschieben oder zu ändern, prüft die CEE CAVA-Lösung diese Dateien nicht auf Viren.

Einrichten von CEE CAVA für NAS-Server

Führen Sie zur Implementierung einer CEE CAVA-Lösung für NAS-Server diese Aufgaben durch:

- Konfigurieren des Domainbenutzerkontos
- Konfigurieren der Virenschutzparameter
- Installieren von Virenschutzsoftware von Drittanbietern
- Installieren von CEE CAVA
- Starten der CEE-Virenschutz-Engine

Konfigurieren des Domainbenutzerkontos

Für die CEE CAVA-Installation ist ein Windows-Benutzerkonto erforderlich, bei dem die Unity-NAS-Server erkennen, dass es über das Unity-Virenprüfrecht verfügt. Dieses Benutzerkonto ermöglicht NAS-Servern die Unterscheidung zwischen CEE CAVA-Anforderungen und anderen Clientanforderungen.

Führen Sie zur Konfiguration des Domainbenutzerkontos folgende Aufgaben durch:

1. Erstellen des Domainbenutzerkontos
2. Erstellen der lokalen Virenschutzgruppen
3. Konfigurieren von Virenprüfrechten auf jedem NAS-Server

Erstellen des Domainbenutzerkontos

Info über diese Aufgabe

So erstellen Sie ein Active Directory-Domainbenutzerkonto für den Virenschutzbenutzer:

Schritte

1. Melden Sie sich bei einem Domain-Controller mit Windows Server Version 2008 SP2 bis 2016 als Domainadministrator an.
2. Wählen Sie in der Systemsteuerung **Verwaltungstools** > **Active Directory-Benutzer und -Computer** aus.
3. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Benutzer** und wählen Sie dann **Neu** > **Benutzer** aus.
4. Geben Sie im Dialogfeld **Neues Objekt - Benutzer** den Vor-, Nach- und Benutzeranmeldenamen für den neuen Benutzer ein und klicken Sie dann auf **Weiter**.
5. Im Dialogfeld **Passwort**:
   a. Geben Sie das Passwort ein und bestätigen Sie es.
   b. Wählen Sie **Passwort läuft nie ab**.
   c. Klicken Sie auf **Next** und dann auf **Finish**.

Erstellen der lokalen Virenschutzgruppen

Info über diese Aufgabe

Erstellen Sie eine lokale Gruppe für jeden NAS-Server in der Domain und fügen Sie der Gruppe den neuen Virenschutzbenutzer hinzu, den Sie im vorherigen Abschnitt erstellt haben.

ANMERKUNG: Wenn Sie den Virenschutzbenutzer den Domainadmins nicht hinzugefügt haben, fügen Sie den Virenschutzbenutzer auf jedem Virenschutzserver der lokalen Gruppe „Administratoren“ hinzu.

Schritte

1. Doppelklicken Sie unter **Active Directory-Benutzer und -Computer** auf **EMC NAS-Server** und klicken Sie auf **Computer**.
2. Klicken Sie im Fenster **Computer** mit der rechten Maustaste auf den NAS-Server und wählen Sie **Verwalten**.
3. Doppelklicken Sie im Fenster **Computerverwaltung** unter **Systemprogramme** auf **Lokale Benutzer und Gruppen**.
4. Klicken Sie mit der rechten Maustaste auf **Gruppen** und wählen Sie **Neue Gruppe** aus.
5. Geben Sie im Dialogfeld **Neue Gruppe** einen Gruppennamen (beispielsweise „viruscheckers“) und eine Beschreibung der Gruppe ein und klicken Sie auf **Hinzufügen**.
6. Im Dialogfeld **Benutzer, Computer, Servicekonten oder Gruppen auswählen**:
   a. Geben Sie den Namen des Virenschutzbenutzerkontos ein, das Sie im vorherigen Abschnitt erstellt haben.
   b. Klicken Sie auf **Namen überprüfen**.
   c. Klicken Sie auf **OK**, um das Dialogfeld **Benutzer, Computer oder Gruppen auswählen** zu schließen, und klicken Sie dann auf **OK**, um zum Dialogfeld **Neue Gruppe** zurückzukehren.
7. Klicken Sie auf **Erstellen** und dann auf **Schließen**.
   Die Gruppe wird erstellt und zur Gruppenliste hinzugefügt.

Konfigurieren von Virenprüfrechten auf jedem NAS-Server

Info über diese Aufgabe

Weisen Sie der neuen lokalen Gruppe Unity-Virenprüfrechte zu.

ANMERKUNG: Sie können mit Microsoft Windows-Tools für die Einstellung der lokalen Policy keine Benutzerrechtzuweisungen für ein Unity-Dateisystem verwalten, da Sie mit diesen Tools Benutzerrechtzuweisungen nicht remote verwalten können.

Schritte

1. Wählen Sie in der Systemsteuerung **Verwaltungstools** > **EMC Unity VNX VNXe NAS-Management** aus.
2. Wenn der NAS-Server bereits ausgewählt ist (Name wird hinter **Data Mover/NAS-Server-Management** angezeigt), fahren Sie mit Schritt 4 fort.
3. Falls der NAS-Server nicht ausgewählt ist:
   a. Klicken Sie mit der rechten Maustaste auf **Data Mover/NAS-Server-Management** und wählen Sie dann **Mit Data Mover/NAS-Server verbinden** aus.
   b. Wählen Sie im Dialogfeld **Data Mover/NAS-Server auswählen** den NAS-Server aus. Wählen Sie hierzu entweder die Domain aus dem Listenfeld **Suchen in:** und anschließend den NAS-Server aus der Liste aus oder geben Sie den Computernamen, die IP-Adresse oder den NetBIOS-Namen des NAS-Servers in das Feld **Name** ein.
4. Doppelklicken Sie auf **Data Mover/NAS-Server-Management** und doppelklicken Sie dann auf **Data Mover/NAS-Server-Sicherheitseinstellungen**.
5. Klicken Sie auf **Zuweisung von Benutzerrechten** und doppelklicken Sie im rechten Fenster auf **EMC Virenprüfung**.
6. Klicken Sie im Dialogfeld **Einstellungen für Sicherheitsrichtlinien** auf **Hinzufügen**.
7. Im Fenster **Benutzer oder Gruppen auswählen**:
   a. Wählen Sie den NAS-Server aus dem Feld **Suchen in:** aus.
   b. Wählen Sie die Virenschutzgruppe aus, die Sie in Schritt Erstellen der lokalen Virenschutzgruppen erstellt haben.
   c. Klicken Sie auf **Hinzufügen** und dann auf **OK**, um zum Dialogfeld **Einstellungen für Sicherheitsrichtlinien** zurückzukehren.
8. Klicken Sie auf **OK**.
   Die Virenprüf-Policy zeigt jetzt die lokale Gruppe für Dateisysteme. Obwohl es sich bei diesem Recht um ein lokales Recht und kein Domainrecht handelt, unterscheidet es dennoch Virenschutzbenutzer von anderen Domainbenutzern.
9. Weisen Sie dem Virenschutzbenutzerkonto auf jedem Host, auf dem Virenschutz-Engine-Software ausgeführt wird, also jedem Virenschutzserver, lokale Administratorrechte zu.

   ANMERKUNG: Wenn es sich beim Virenschutzserver um einen Domain-Controller handelt, muss das Virenprüfbenutzerkonto der Domainadministratorgruppe statt der lokalen Administratorgruppe hinzugefügt werden, da die lokale Administratorgruppe nicht auf einem Domain-Controller verwaltet wird.

   Für jeden Virenschutzserver in der Domain:
   a. Wählen Sie in der Systemsteuerung **Verwaltungstools** > **Computerverwaltung** aus.
   b. Wählen Sie im Menü **Aktion** des Fensters **Computerverwaltung** die Option **Verbindung mit anderem Computer herstellen** aus.
   a. Wählen Sie im Fenster **Computer auswählen** den Virenschutzserver aus und klicken Sie dann auf **OK**.
   b. Im Fenster **Computerverwaltung**:
      i. Blenden Sie **Systemprogramme** ein.
      ii. Blenden Sie **Lokale Benutzer und Gruppen** ein.
      iii. Klicken Sie auf **Gruppen**.
   c. Klicken Sie mit der rechten Maustaste auf die Gruppe **Administratoren**, fügen Sie das Domainvirenschutzbenutzerkonto hinzu und wählen Sie dann **Eigenschaften** aus.
   d. Klicken Sie im Fenster **Kontoeigenschaften** auf die Registerkarte **Mitglieder von** und klicken Sie auf **Hinzufügen**.
   e. Geben Sie im Dialogfeld **Gruppen auswählen** im Feld **Geben Sie die zu verwendenden Objektnamen ein** **Administratoren** ein, und klicken Sie auf **OK**.
   f. Klicken Sie auf **OK**, um das Dialogfeld **Kontoeigenschaften** zu schließen.

Konfigurieren der Virenschutzparameter

In diesem Thema werden die Schritte zur Konfiguration der Virenschutzparameter aufgeführt.

Schritte

1. Wählen Sie in der Systemsteuerung **Verwaltungstools** > **EMC Unity VNX VNXe NAS-Management** aus.
2. Blenden Sie in der Konsolenstruktur den Data Mover/NAS-Server-Management-Node ein (bei einem Unity-System stehen die Einträge für die NAS-Server).

   Der Virenschutz-Node wird in der Konsolenstruktur angezeigt. Der Status des Virenschutzservice für den ausgewählten NAS-Server lautet entweder „Gestoppt“ oder „Wird ausgeführt“.

   ANMERKUNG: Wenn Sie keinen NAS-Server ausgewählt haben, müssen Sie einen Server auswählen, bevor Sie das Virenschutz-Management-Snap-in verwenden können. Wenn ein NAS-Server ausgewählt ist, wird sein Name neben dem Data Mover/NAS-Server-Management-Node in der Konsolenstruktur angezeigt.

3. Klicken Sie auf den Virenschutzknoten.

   Die Liste der Parametereinstellungen wird im Detailfenster angezeigt.
4. Im Detailfenster:
   a. Klicken Sie auf den Parameter, den Sie ändern möchten, und wählen Sie dann **Eigenschaften** aus.
   Das Dialogfeld **Eigenschaften** für diesen Parameter wird angezeigt. Eine Beschreibung der Parameter finden Sie hier: Konfigurierbare Virenschutzknoten-Parameter.
   b. Wenn der Parameter mehrere Einstellungen umfasst, geben Sie die Werte für die Einstellungen ein, klicken Sie auf **Hinzufügen** und dann auf **OK**.
   c. Wenn der Parameter eine einzige Einstellung umfasst, geben Sie den Wert für die Einstellung ein und klicken Sie dann auf **OK**.

Konfigurierbare Virenschutzknoten-Parameter

Für Unity-Systeme können Sie entweder eine Virenschutzkonfigurationsdatei in Unisphere erstellen oder Sie können eine Virenschutzkonfigurationsdatei hochladen, die Sie offline erstellen. So greifen Sie auf die Virenschutzkonfiguration in Unisphere zu:

1. Wählen Sie unter **Speicher** die Optionen **Datei** > **NAS-Server** aus.
2. Wählen Sie den entsprechenden NAS-Server und wählen Sie dann das Symbol **Bearbeiten** aus.
3. Wählen Sie die Registerkarte **Sicherheit** aus.

Die folgende Tabelle beschreibt die Parameter, die Sie in der Datei `viruschecker.conf` konfigurieren oder mit dem EMC Unity/VNX/VNXe-NAS-Management-Snap-in verwenden können.

ANMERKUNG: Der Parameter masks= kann die Performance der Virenprüfung erheblich beeinträchtigen. Es wird empfohlen, dass Sie masks=*.* nicht verwenden, weil diese Einstellung alle Dateien scannt. Viele Dateien können keine Viren enthalten, daher ist masks=*.* keine effiziente Einstellung. Die meisten Virenschutz-Engines scannen nicht alle Dateien. Die Parameter masks= und excl= in der Datei viruschecker.conf müssen gleich oder eine Obermenge der Einstellungen masks= und excl= sein, die von der Virenschutz-Engine verwendet werden.

Tabelle 7. Parameter in der Datei viruschecker.conf

Parameter	Beschreibung	Beispiel
`httpport=`	HTTP-Portnummer auf der CEE-Maschine, die das Speichersystem verwendet. **ANMERKUNG:** Wenn Sie den Parameter httpport= festlegen, müssen Sie dieselbe Portnummer im Eintrag HttpPort der Windows Registry angeben unter: `HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\Configuration`	`httpport=12228`

Tabelle 7. Parameter in der Datei viruschecker.conf (fortgesetzt)

Parameter	Beschreibung	Beispiel

`masks=`	Konfiguriert Dateierweiterungen, die gescannt werden.	`masks=*.exe`
		Im folgenden Beispiel werden nur EXE-, COM-, DOC-, DOCX- und PPT-Dateien gescannt:
		`masks=*.exe:*.com:*.doc:*.docx:*.ppt`

`excl=`	Definiert von der Prüfung auszuschließende Dateien oder Dateierweiterungen.	`excl=pagefile.sys:*.tmp`
`addr=`	Legt die IP-Adressen für die Virenschutzgeräte oder einen vollständig qualifizierten Domainnamen fest. **ANMERKUNG:** Die Verwendung von lokalen Linknetzwerkadressen zur Definition von Virenschutzgeräten wird nicht unterstützt.	Einzelne IP-Adresse: `addr=192.16.20.29` Mehrere IP-Adressen: `addr=192.16.20.15:192.16.20.16 :[2510:0:175:111:0:4:aab:ad2]:[2510:0:175:111:0:4:aab:a6f]:192.16.20.17` **ANMERKUNG:** IPv6-Adressen müssen in eckige Klammern gesetzt werden, um sie von dem Doppelpunkttrennzeichen zu trennen, das zwischen mehreren Adressen verwendet wird. Vollständig qualifizierter Domainname: `addr=wichita.nasdocs.emc.com` **ANMERKUNG:** Wenn ein Virenschutzgerät vorübergehend oder dauerhaft entfernt wird, löschen Sie seine IP-Adresse aus dieser Datei, bevor Sie den CAVA-Service herunterfahren.
`CIFSserver=<CIFS_server_name>` (optional)	Identifiziert die Schnittstelle auf dem NAS-Server, die von dem CAVA-Client `<CIFS_server_name>` (NetBIOS-Name, Rechnername oder IP-Adresse) des SMB/CIFS-Servers auf dem NAS-Server verwendet wird. Wenn der Parameter nicht angegeben ist, verwendet der NAS-Server den ersten SMB/CIFS-Server, den er findet. **ANMERKUNG:** Die Verwendung von lokalen Linknetzwerkadressen zur Definition von Virenschutzgeräten wird nicht unterstützt.	`CIFSserver=CIFS_Host2`
`maxsize=<n>` (optional)	Legt die maximale Größe für zu überprüfende Dateien fest. Dateien, die größer sind, werden nicht geprüft. Geben Sie eine Hexadezimalzahl mit dem Präfix 0x ein. Die maximale Größe muss kleiner oder gleich 0xFFFFFFFF sein. Wenn der Parameter nicht angegeben oder gleich 0 ist, bedeutet dies, dass keine Dateigrößenbeschränkung festgelegt ist.	`maxsize=0xFFFFFFFF`

Tabelle 7. Parameter in der Datei viruschecker.conf (fortgesetzt)

Parameter	Beschreibung	Beispiel
	Die Dateigröße ist in Bytes mit maximal 4 GB angegeben.	
`highWaterMark=<n>` (optional)	Bearbeitet den Parameter highWaterMark. Wenn die Anzahl der Anfragen über highWaterMark liegt, wird ein Protokollereignis an das Speichersystem gesendet. Der Standardwert ist 200. Das Maximum ist 0xFFFFFFFF.	`highWaterMark=200`
`lowWaterMark=<n>` (optional)	Bearbeitet den Parameter lowWaterMark. Wenn die Anzahl der Anfragen unter lowWaterMark liegt, wird ein Protokollereignis an Unity gesendet. Der Standardwert ist 50.	`lowWaterMark=50`
`waitTimeout=<n>` (optional)	Legt die maximale Zeit in Millisekunden fest, die ein Client blockiert sein kann, während der Client versucht, auf eine Datei zuzugreifen, die gescannt wird. Der Standardwert ist 0 Millisekunden, was darauf hinweist, dass der Clientzugriff blockiert wird, bis die Datei gescannt wurde. Die Einstellung dieses Parameters hat keinen Einfluss auf das tatsächliche Scannen der Datei.	`waitTimeout=0 milliseconds`
`RPCRetryTimeout=<n>` (optional)	Legt das Timeout der RPC-Wiederholung fest. Das Timeout wird in Millisekunden angegeben. Der Standardwert ist 5.000 Millisekunden. Das Maximum ist 0xFFFFFFFF.	`RPCRetryTimeout=4000 milliseconds`
`RPCRequestTimeout=<n>` (optional)	Legt das Timeout der RPC-Anforderung (in Millisekunden) fest. Funktioniert mit RPCRetryTimeout. Wenn ein RPC an das Virenschutzgerät gesendet wird, versucht der NAS-Server, falls der Server nach dem RPCRetryTimeout antwortet, die Anforderung erneut, bis RPCRequestTimeout erreicht ist. Wenn RPCRequestTimeout erreicht ist, wechselt der NAS-Server zum nächsten verfügbaren Virenschutzgerät. Der Standardwert ist 25.000 Millisekunden. **ANMERKUNG:** Dieser Wert muss größer sein als der Wert für Symantec Protection Engine Container File Processing Limits.	`RPCRequestTimeout=20000 milliseconds`
`msrpcuser=` (optional)	Gibt den Namen an, der entweder einem einfachen Benutzerkonto zugewiesen ist oder einem Benutzerkonto, das	Benutzerkonto: `msrpcuser=user1`

Tabelle 7. Parameter in der Datei viruschecker.conf (fortgesetzt)

Parameter	Beschreibung	Beispiel
	Teil einer Domain ist, unter der der CAVA-Service auf der CEE-Maschine ausgeführt wird.	Domain\Benutzerkonto: `msrpcuser=CEE1\user1`
`surveyTime=<n>` (optional)	Gibt das Zeitintervall an, in dem alle Virenschutzgeräte gescannt werden, um zu sehen, ob sie online oder offline sind. Dieser Parameter arbeitet mit dem Parameter für das Herunterfahren, der als Nächstes gezeigt wird. Wenn kein Virenschutzgerät antwortet, beginnt der Prozess des Herunterfahrens mithilfe des konfigurierten Parameters für das Herunterfahren. Dies ist der einzige Parameter, der das Herunterfahren auslöst. Der Standardwert ist 10 Sekunden. min=1, max=3.600.	`surveyTime=60 seconds`
`shutdown=`	Gibt an, welche Aktion zum Herunterfahren erfolgen soll, wenn kein Server zur Verfügung steht. Funktioniert mit dem Parameter surveyTime. Optionen umfassen die folgenden Parameter: • `shutdown=cifs` : Beendet SMB/CIFS, wenn kein Virenschutzgerät zur Verfügung steht. (Windows-Clients können nicht auf Unity-Shares zugreifen.) Wenn die strenge Datensicherheit in der Umgebung eine wichtige Rolle spielt, müssen Sie diese Option aktivieren, um den Zugriff auf die Dateien zu verhindern, wenn kein Virenschutzgerät verfügbar ist. Wenn diese Option nicht aktiviert ist und kein Virenschutzgerät verfügbar ist, können Clients Dateien ohne Virenprüfung ändern. **ANMERKUNG:** Shutdown=CIFS muss deaktiviert sein, wenn weniger als zwei Virenschutzgeräte konfiguriert sind.	`shutdown=cifs`
	• `shutdown=no` : Liste der Virenschutzgeräte wird weiterhin verwendet, wenn kein Virenschutzgerät zur Verfügung steht. Es existieren zwei Marken (niedrig und hoch). Wenn einer dieser Werte erreicht wird, wird ein Ereignisprotokoll gesendet. Verwenden Sie das Ereignisprotokoll, um Korrekturmaßnahmen auf dem NAS-Server vorzunehmen und	`shutdown=no`

Tabelle 7. Parameter in der Datei viruschecker.conf (fortgesetzt)

Parameter	Beschreibung	Beispiel
	damit sicherzustellen, dass die Virenprüfung funktionsfähig ist.	
	• `shutdown=viruschecking` : Beendet die Virenprüfung, wenn kein Virenschutzgerät zur Verfügung steht. (Windows-Clients können ohne Virenprüfung auf Unity-Shares zugreifen.) Der Standardwert ist shutdown=no.	`shutdown=viruschecking`

Installieren von Virenschutzsoftware von Drittanbietern

Sie müssen ein unterstütztes Virenschutzsoftware-Paket eines Drittanbieters (Virenschutz-Engine) auf jedem Host in der Domain installieren, der als Virenschutzserver fungieren soll. Damit Dateien weiterhin geprüft werden, wenn ein Virenschutzserver ausfällt oder vom Unity-NAS-Server nicht erreicht werden kann, müssen Sie mindestens zwei Virenschutzserver in der Domain konfigurieren. Die aktuelle Liste der unterstützten Virenschutz-Engines und Virenschutzversionen erhalten Sie im E-Lab™ Interoperability Navigator auf der Supportwebsite.

Sie müssen alle unterstützten Virenschutzsoftwarepakete von Drittanbietern mit Ausnahme des Trend MicroServerProtect-Pakets auf einem Host installieren, bevor Sie CEE CAVA auf einem Host installieren. Wenn Sie Trend MicroServerProtect-Virenschutzsoftware auf einem Host installieren möchten, installieren Sie zunächst CEE CAVA wie in Installieren von CEE CAVA beschrieben.

Weitere Informationen zur Installation von Virenschutzsoftware von Drittanbietern finden Sie unter *Verwenden des Common Event Enabler auf Windows-Plattformen*.

Installieren von CEE CAVA

Dieses Thema bietet wichtige Informationen zur Installation von CAVA.

Sie müssen CEE CAVA auf jedem Host in der Domain installieren, der als Virenschutzserver fungieren soll. Installationsanweisungen finden Sie unter *Verwenden des Common Event Enabler auf Windows-Plattformen* auf Online Support. Wählen Sie während der Ausführung des Installationsassistenten, wenn Sie im Schritt „Installationstyp“ nur CAVA statt der vollständigen CEE-Software installieren möchten, **Benutzerdefiniert** und dann **CAVA** aus und klicken Sie auf **Weiter**.

Öffnen Sie nach der Installation von CEE CAVA `Services.msc` auf jedem Virenschutzserver, ändern Sie den CAVA-Service auf „Anmelden“ und führen Sie den Service mithilfe des Domainvirenschutzkontos aus.

Entfernen alter Versionen von CEE CAVA

Wenn auf einem Virenschutzserver eine vorherige Version von CEE CAVA installiert ist, entfernen Sie diese Version von CEE CAVA, starten Sie den Server neu und installieren Sie dann die neue Version von CEE CAVA. Entfernen Sie im Fenster **Programme hinzufügen/entfernen** der Windows-Systemsteuerung alte Versionen von CEE CAVA. Sie müssen über lokale Administratorrechte verfügen, um Programme zu entfernen.

ANMERKUNG: Wenn Sie die vorherige Version vor dem Upgrade von CEE CAVA nicht entfernen, können Sie auf der Seite für die Erstinstallation die Option „Entfernen“ wählen, um die vorherige Version zu entfernen. Fahren Sie dann mit der Installation fort.

Erneute Installation von CEE CAVA

Bei der erneuten Installation von CEE CAVA wird eventuell eine Meldung zum Schutz vor Überschreiben angezeigt, wenn die Installationsdateien im temporären Verzeichnis entpackt wurden. Wenn diese Meldung angezeigt wird, klicken Sie im Fenster „Überschreibschutz“ auf „Ja zu allem“**,** um die vorhandenen Dateien zu überschreiben. Dieser Prozess sorgt dafür, dass sich die aktuelle Version der Dateien im temporären Verzeichnis befindet.

Starten der CEE-Virenschutz-Engine

In diesem Thema werden die Schritte zum Starten der CEE-Virenschutz-Engine (Virenprüfagent) in Unisphere aufgeführt.

Schritte

1. Greifen Sie auf Unisphere zu.
2. Wählen Sie unter **Speicher** die Optionen **Datei** > **NAS-Server** aus.
3. Wählen Sie den entsprechenden NAS-Server und wählen Sie dann das Symbol **Bearbeiten** aus.
4. Wählen Sie auf der Registerkarte **Sicherheit** die Unterregisterkarte **Virenschutz** aus.
5. Wählen Sie **Virenschutzservice aktivieren** aus.
6. Wählen Sie **Abrufen der aktuellen Konfiguration** aus, um die aktuelle CAVA-Konfigurationsdatei zu erhalten. Speichern Sie sie lokal als `cava.conf`. Beim ersten Mal, dass Sie diese Datei abrufen, ist es eine leere Vorlage mit Kommentaren neben jedem Feld.
7. Bearbeiten Sie die Datei `cava.conf` nach Bedarf. Beim ersten Mal, dass Sie diese Datei bearbeiten, entfernen Sie die Kommentare und geben Sie die CAVA-Parameter (z. B. die Liste der CAVA-Server) in dieser Datei an.
8. Wählen Sie **Upload der neuen Konfiguration** aus und laden Sie die neue Konfiguration auf den NAS-Server hoch.

Ergebnisse

Der Virenschutzstatus ändert sich zu `Virenschutz wird ausgeführt`.

ANMERKUNG: Wenn der `shutdown`-Virenschutz-Node-Parameter auf `no` festgelegt wird, bedeutet der Status „Wird ausgeführt“ nicht automatisch, dass der Virenschutz funktioniert. Klicken Sie auf **Ereignisse** > **Warnmeldungen**, um zu überprüfen, ob die Virenschutzserver online sind. Um Probleme mit dem Clientzugriff zu vermeiden, vergewissern Sie sich, dass auf alle Virenschutzserver zugegriffen werden kann und es keine Probleme mit der Konfiguration gibt. Weitere Informationen zum `shutdown`-Virenschutz-Node-Parameter oder zu anderen zugehörigen Parametern finden Sie unter Konfigurierbare Virenschutzknoten-Parameter.

5

Verwenden der CEE-Ereignisveröffentlichung mit Unity

Dieses Kapitel umfasst folgende Themen:

Themen:

Übersicht über Ereignisveröffentlichung

Der Common Event Enabler (CEE) stellt eine Lösung zur Ereignisveröffentlichung (Common Event Publishing Agent) für Unity-Clients bereit, die es Anwendungen von Drittanbietern erlaubt, sich zu registrieren, um beim Zugriff auf Dateisysteme Ereignisbenachrichtigungen und Kontextinformationen vom Speichersystem zu erhalten. Der Ereignisveröffentlichungsagent (CEPA) liefert der Anwendung sowohl eine Ereignisbenachrichtigung als auch zugehörigen Kontext in einer Nachricht. Der Kontext kann aus Metadaten der Datei oder Verzeichnismetadaten bestehen, die erforderlich sind, um die Unternehmens-Policy zu entscheiden. Um den Ereignisveröffentlichungsagenten zu verwenden, müssen Sie ein Unity-System mit mindestens einem im Netzwerk konfigurierten NAS-Server haben.

Sie müssen mindestens eine Ereignisoption definieren (vor dem Ereignis, nach dem Ereignis oder Fehlerfolgeereignis), wenn Ereignisveröffentlichung aktiviert ist:

- Vor-Ereignis-Benachrichtigungen werden gesendet, bevor eine SMB-Clientanforderung verarbeitet wird.
- Nach-Ereignis-Benachrichtigungen werden nach einer erfolgreichen SMB-Clientanforderung gesendet.
- Fehlerfolgeereignis-Benachrichtigungen werden nach einer fehlgeschlagenen SMB-Clientanforderung gesendet.

Tabelle 8. Ereignisbeschreibungen

Wert	Definition
`OpenFileNoAccess`	Sendet eine Benachrichtigung, wenn eine Datei für eine Änderung, die kein Lese- oder Schreibzugriff ist (z. B. Lese- oder Schreibattribute auf der Datei) geöffnet wird.
`OpenFileRead`	Sendet eine Benachrichtigung, wenn eine Datei für den Lesezugriff geöffnet wird.
`OpenFileReadOffline`	Sendet eine Benachrichtigung, wenn eine Offlinedatei für den Lesezugriff geöffnet wird.
`OpenFileWrite`	Sendet eine Benachrichtigung, wenn eine Datei für den Schreibzugriff geöffnet wird.
`OpenFileWriteOffline`	Sendet eine Benachrichtigung, wenn eine Offlinedatei für den Schreibzugriff geöffnet wird.
`OpenDir`	Sendet eine Benachrichtigung, wenn ein Verzeichnis geöffnet wird.
`CreateFile`	Sendet eine Benachrichtigung, wenn eine Datei erstellt wird.
`CreateDir`	Sendet eine Benachrichtigung, wenn ein Verzeichnis erstellt wird.
`DeleteFile`	Sendet eine Benachrichtigung, wenn eine Datei gelöscht wird.
`DeleteDir`	Sendet eine Benachrichtigung, wenn ein Verzeichnis gelöscht wird.
`CloseModified`	Sendet eine Benachrichtigung, wenn eine Datei vor dem Schließen geändert wird.
`CloseUnmodified`	Sendet eine Benachrichtigung, wenn eine Datei vor dem Schließen nicht geändert wird.
`CloseDir`	Sendet eine Benachrichtigung, wenn ein Verzeichnis geschlossen wird.
`RenameFile`	Sendet eine Benachrichtigung, wenn eine Datei umbenannt wird.

Tabelle 8. Ereignisbeschreibungen (fortgesetzt)

Wert	Definition
`RenameDir`	Sendet eine Benachrichtigung, wenn ein Verzeichnis umbenannt wird.
`SetAclFile`	Sendet eine Benachrichtigung, wenn die Sicherheitsbeschreibung (ACL) für eine Datei geändert wird.
`SetAclDir`	Sendet eine Benachrichtigung, wenn die Sicherheitsbeschreibung (ACL) für ein Verzeichnis geändert wird.

Einschränkungen und Grenzen der Ereignisveröffentlichung

Bevor Sie beginnen

Bevor Sie Ereignisveröffentlichung für einen NAS-Server einrichten können:

- Sie können keine Ereignisveröffentlichung für einen NAS-Server aktivieren, der als Replikationsziel fungiert.
- Es muss mindestens ein Dateisystem für den NAS-Server vorhanden sein.
- Sie müssen die IP-Adressen der CEPA-Server abrufen.
- Stellen Sie sicher, dass Ereignisbenachrichtigungen für das SMB-Protokoll im Fenster **Dateisysteme Eigenschaften Erweitert** aktiviert wurden.

CEPA-Speicherpools

In Unity-Systemen:

- Für Folgeereignisse und Fehlerfolgeereignisse können Sie bis zu drei CEPA-Speicherpools definieren.
- Für Vor-Ereignis-Benachrichtigungen können Sie nur einen CEPA-Speicherpool definieren.

CEPA-Server

Jeder NAS-Server muss einen CEPA-Speicherpool angeben, der aus mindestens zwei CEPA-Servern besteht.

Installieren von CEE CEPA

Installationsanweisungen finden Sie unter *Verwenden des Common Event Enabler auf Windows-Plattformen* auf Online Support. Wählen Sie während der Ausführung des Installationsassistenten, wenn Sie im Schritt „Installationstyp“ nur CEPA statt der vollständigen CEE-Software installieren möchten, **Benutzerdefiniert** und dann **CEPA** aus und klicken Sie auf **Weiter**.

Einrichten von Ereignisveröffentlichung

Info über diese Aufgabe

Sie können mithilfe der Unisphere GUI die Ereignisveröffentlichung pro NAS-Server einrichten.

- Sie können keine Ereignisveröffentlichung für einen NAS-Server aktivieren, der als Replikationsziel fungiert.
- Es muss mindestens ein Dateisystem für den NAS-Server vorhanden sein.
- Sie müssen die IP-Adressen der CEPA-Server abrufen.

Schritte

1. Wählen Sie unter **Speicher** die Optionen **Datei** > **NAS-Server** aus.
2. Wählen Sie den entsprechenden NAS-Server und wählen Sie dann das Symbol **Bearbeiten** aus.

3. Wählen Sie auf der Registerkarte **Schutz und Ereignisse** die Unterregisterkarte **Ereignisveröffentlichung** aus.
4. Aktivieren Sie das Kontrollkästchen **Common Event Publishing aktivieren**.
5. Geben Sie im Fenster **Neuer Ereignispool** die erforderlichen Elemente an. Sie müssen mindestens ein Ereignis aus einer der verfügbaren Kategorien (vor dem Ereignis, nach dem Ereignis oder Fehlerfolgeereignis) konfigurieren.
6. Klicken Sie auf **Konfigurieren**.
7. Wählen Sie optional **Policy-Einstellungen anzeigen** aus, um die Policies für Fehler vor und nach Ereignissen zu konfigurieren.
8. Wählen Sie optional **Erweiterte Einstellungen anzeigen** aus, um die CEPA-Serveroptionen zu konfigurieren.
9. Klicken Sie auf **Anwenden**, nachdem Sie die Konfiguration der Ereignisse abgeschlossen haben.

Nächste Schritte

Sobald Sie Ereignisveröffentlichung für einen NAS-Server eingerichtet haben, können Sie sie optional für jedes zugeordnete Dateisystem aktivieren. Wählen Sie dafür **SMB-Ereignisveröffentlichung aktivieren** auf der Registerkarte **Erweitert** auf der Eigenschaftenseite des Dateisystems aus.