Sao lưu và khôi phục hệ thống Domain

Mục tiêu bài học

- Giám sát Active Directory
- Quản trị CSDL Active Directory
- Active Directory Recycle Bin
- Sao lưu và khôi phục AD DS và Domain Controllers

Tìm hiểu về hiệu năng và nghẽn

Các tài nguyên chính của hệ thống

- CPU
- Disk
- Memory
- Network

Nghẽn: 1 tài nguyên ở trạng thái hoạt động cao điểm

Các công cụ giám sát

Task Manager

Giám sát thời gian thực các thành phần chính của hệ thống

Event Viewer

Giám sát được lưu lại của các dịch vụ hệ thống khác nhau

Resource Monitor

Giám sát thời gian thực chi tiết về việc sử dụng tài nguyên

Reliability Monitor

Kiểm tra khả năng tin cậy của hệ thống theo thời gian

Performance Monitor

Giám sát hiệu năng hệ thống trong quá khứ cũng như thời gian thực

Performance Monitor

Các chỉ số hữu ích trong bất cứ một server baseline nào

- Memory \ Pages/sec
- PhysicalDisk \ Avg. Disk Queue Length
- Processor \ %Processor Time

Các chỉ số hữu ích cho việc giám sát Active Directory

- NTDS\ DRA Inbound Bytes Total/sec
- NTDS\ DRA Inbound Object
- NTDS\ DRA Outbound Bytes Total/sec
- NTDS\ DRA Pending Replication Synchronizations
- NTDS \ Kerberos Authentications/sec
- NTDS\ NTLM Authentications

Các bộ thu thập dữ liệu

Thu thập thông tin dữ liệu

- Chỉ số hiệu năng
- Dữ liệu lưu vết sự kiện
- Thông tin cấu hình hệ thống (các key trong registry)

Các kịch bản sử dụng:

- Xem hiệu năng thời gian thực với Performance Monitor
- Tạo 1 log (tự tạo hoặc theo lịch) và sau đó xem Reports
- Tạo các cảnh báo dựa trên các ngưỡng (threshold)
- Sử dụng bởi các ứng dụng khác

Để tạo 1 bộ thu thập dữ liệu:

- Bắt đầu từ 1 template; các template role thêm bởi Windows
- Lưu các giá trị hiện tại của các chỉ số trong 1 cửa sổ Performance Monitor
- Tự xác định và cấu hình các lựa chọn dữ liệu trong 1 bộ
- Export/import dự liệu thu thập ra XML

Các bước thực thi giám sát tốt nhất

1. Giám sát sớm để tạo baseline
   - Ghi lại thông tin hiệu năng khi hệ thống đang hoạt động tốt
   - Ghi lại chỉ số của server và các chức năng trong thời gian hệ thống rảnh và bận
2. Giám sát thường xuyên để xác định các sự cố có thể xảy ra
   - So sánh với baseline và kiểm tra độ sai lệch
3. Cần biết làm thế nào để giám sát và hiểu được chỉ số hiệu năng trước khi có sự cố
   - Thiết lập các bộ thu thập dữ liệu
   - Xây dựng các kỹ năng để hiểu các chỉ số hiệu năng
4. Thu thập một cách hợp lý
   - Không nên thu thấp quá nhiều thông tin
     - Làm giảm hiệu năng
     - Tạo ra các "nhiễu", làm cho khó phân biệt được với các sự cố thực

Active Directory Best Practices Analyzer

Công cụ mới trong Windows Server 2008 R2 giúp người quản trị phát hiện các vi phạm các thực thi tốt nhất và giúp triển khai các thực thi tốt nhất

cho:

- AD DS
- AD CS
- DNS Server
- Terminal Services

NTDSUtil

Quản trị và điều khiển các hoạt động single master

Thực hiện duy trì CSDL AD DS

- Thực hiện chống phân mảnh offline
- Tạo và mount các snapshot
- Chuyển các file CSDL

Làm sạch dữ liệu domain controller

- Xóa hoặc giáng cấp Domain controller trong khi chưa kết nối với domain

Đặt lại mật khẩu của Directory Services Restore Mode

- set dsrm

Active Directory Domain Services có khả năng khởi động lại

- Tính năng mới trong Windows Server 2008
- AD DS có thể được khởi động và dừng lại bằng việc sử dụng Services console
- AD DS có thể có 3 trạng thái:
  - AD DS Started
  - AD DS Stopped
  - Directory Services Restore Mode (DSRM)
- Sẽ không thể thực hiện khôi phục trạng thái hệ thống trong khi AD DS đang ở trạng thái Stopped

Thực hiện duy trì CSDL

Thu gom "rác"

Rác: loại bỏ các mục đã bị xóa khi đủ lâu mà không cần khôi phục

Chống phân mảnh (Defragmentation)

Online defragmentation (là 1 phần của việc thu gom rác): Lấy lại các không gian không sử dụng

Offline defragmentation (thủ công): Giải phóng các không gian không sử dụng và giảm kích thước của file

- Sử dụng NTDSUtil
- Lưu ý: phải thực hiện trong chế độ DSRM hoặc dừng AD DS

Active Directory Snapshots

Tạo 1 snapshot cho Active Directory

NTDSUtil

Gắn (Mount) snapshot vào 1 port duy nhất

NTDSUtil

Hiển thị snapshot

Right-click vào điểm root của **Active Directory Users and Computers** và chọn **Connect to Domain Controller**

Nhập serverFQDN:port

Xem (read-only) snapshot

Không thể khôi phục dữ liệu trực tiếp từ snapshot này

Khôi phục dữ liệu

Nhập liệu thủ công hoặc

Khôi phục 1 bản sao lưu từ cùng ngày của snapshot

Khôi phục đối tượng đã bị xóa

Khi 1 đối tượng bị xóa

- Loại bỏ hầu hết các thuộc tính ngoại trừ
  - SID, objectGUID, lastKnownParent, sAMAccountName
- Di chuyển tới Deleted Objects container, đánh dấu isDeleted

Bạn có thể khôi phục các đối tượng bị xóa khi

- Chức năng Domain là Windows Server 2003 hoặc mới hơn
- Đối tượng bị xóa chưa bị thu dọn

Để khôi phụ các đối tượng bị xóa:

- LDP.exe
  - Thay đổi isDeleted
  - Cung cấp tên duy nhất (DN)
- Phục hồi tất cả các thuộc tính khác

Xóa và khôi phục đối tượng từ Active Directory

Các đối tượng bị xóa được khôi phục lại thông qua phục hồi trạng thái

Khi đối tượng bị xóa, hầu hết các thuộc tính bị xóa

Thẩm quyền khôi phục đòi hỏi tạm ngừng AD DS

Active Directory Recycle Bin là gì?

Tính năng mới của Windows Server 2008 R2 Active Directory

Cung cấp 1 cách để khôi phục các đối tượng bị khóa mà không cần ngừng AD DS

Dùng tiện ích LDP.exe hoặc Windows Power Shell với Active Directory Module

Các yêu cầu của Active Directory Recycle Bin

Tính năng này mặc định bị tắt; nó phải được kích hoạt thủ công

Cấp độ chức năng Forest phải là Windows Server 2008 R2

Adprep /forestprep và /domainprep có thể là cần thiết

Kích hoạt bằng thực thi:

```
Enable-ADOptionalFeature –Identity ‘CN=Recycle Bin
Feature,CN=Optional Features,CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration, DC=contoso,DC=com’ –Scope
ForestOrConfigurationSet –Target ‘contoso.com’
```

Các công cụ sao lưu và khôi phục

Windows Server Backup snap-in (sử dụng cục bộ hoặc từ xa)

- Sao lưu hoàn toàn 1 server (tất cả các phần)
- Sao lưu các phần được lựa chọn
- Sao lưu các file nhất định (Windows Server 2008 R2 only)
- Sao lưu trạng thái hệ thống (bao gồm tất cả các phần thiết yếu)
- Khôi phục các phần, thư mục, file, hoặc trạng thái hệ thống

wbadmin.exe

Thực hiện sao lưu thủ công hoặc tự động

Sao lưu vào CD/DVD/HDD

- No tape
- Dùng 1 HDD đã được xác định để sao lưu: Khuyến cáo hoặc bắt buộc

Giới thiệu về sao lưu AD DS and Domain Controller

Bạn phải sao lưu tất cả các phần thiết yếu

- System volume: Phần chưa các file boot
- Boot volume: Phần chưa hệ điều hành và registry của Windows
- Phần lưu trữ SYSVOL, CSDL AD DS (NTDS.dit), logs
- Không lưu các dữ liệu khác trên phần này vì nó sẽ làm tăng thời gian sao lưu và khôi phục

Windows Server Backup (wbadmin.exe)

Các công cụ khác để sao lưu và khôi phục

- Active Directory Snapshots
- Windows PowerShell cmdlets
- Windows Recovery Environment
  - Khởi động Windows Server 2008 từ DVD và lựa chọn System Recovery Options
  - Cài đặt máy cục bộ như 1 lựa chọn khởi động
  - Hữu dụng cho khôi phục toàn bộ hệ thống

Các lựa chọn khôi phục Active Directory

Khôi phục không thẩm quyền (thông thường)

- Khôi phục domain controller về trạng thái tốt được biết trước đây của Active Directory
- Domain controller sẽ đwọc cập nhật bằng việc dùng bản sao lưu chuẩn từ các đối tác cập nhật

Khôi phục có thẩm quyền

- Khôi phục domain controller về trạng thái tốt được biết trước đây của Active Directory
- "Đánh dấu" các đối tượng mà bạn muốn có thẩm quyền
  - Windows thiết lập giá trị phiên bản rất cao
- Domain controller được cập nhật từ các cập nhật của nó
- Domain controller gửi thẩm quyền cập nhật cho các đối tác của nó

Khôi phục toàn bộ Server

- Thường được thực hiện trong Windows Recovery Environment

Khôi phục vị trí thay thế

Khôi phục không thẩm quyền

Khởi động domain controller trong DSRM

- Tại chỗ: Nhấn F8 trong quá trình khởi động
- Từ xa sử dụng remote desktop:
  - Cấu hình khởi động lại trong DSRM: bcdedit /set safeboot dsarepair
  - Khởi động lại: shutdown -t 0 -r

Đăng nhập với tài khoản Administrator và mật khẩu DSRM

Thực hiện khôi phục không thẩm quyền

- Dùng Windows Server Backup (wbadmin.exe) để khôi phục AD DS

Khởi động lại

- Đặt chế độ khởi động lại thông thường: bcdedit /deletevalue safeboot dsarepair
- Khởi động lại: shutdown -t 0 -r

Domain controller sao chép tất cả thay đổi từ ngày sao lưu từ các đối tác của nó

Khôi phục có thẩm quyền

Khởi động lại domain controller ở chế độ DSRM

Đăng nhập bằng tại khoản Administrator và mật khẩu DSRM

Thực hiện khôi phục không thẩm quyền

- Dùng Windows Server Backup (wbadmin.exe) để khôi phục AD DS

Đánh dấu các đối tượng có thẩm quyền

- `restore [object|subtree] "objectDN"`
- Các thay đổi thẩm quyền có phiên bản cao hơn đối tác của nó

Khởi động lại

Khôi phục domain controller sao chép các thay đổi từ ngày sao lưu

Các đối tác thấy các thay đổi thẩm quyền với các phiên ban cao hơn

- Các đối tác kéo các thay đổi thẩm quyền từ domain controller được khôi phục

Tổng kết bài học

Các khái niệm về hiệu năng, nghẽn

Các công cụ giám sát: Task Manager, Event Viewer…

Các bước thực thi giám sát hệ thống

Công cụ Active Directory Best Practices Analyzer

Các file của CSDL AD và duy trì CSDL

Các bản sao (snapshot) của AD

Khôi phục đối tượng bị xóa và tính năng Active Directory Recycle Bin

Các công cụ sao lưu và khôi phục và ứng dụng vào AD